IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SENTILLION, INC.,	)	
	)	
Plaintiff and Counterclaim-Defendant,	)	
	)	
v.	)	C.A. No. 06-13 (SLR)
	)	
CAREFX CORP.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant and Counterclaim-Plaintiff.	)	

NOTICE OF DEPOSITION OF DUKE UNIVERSITY MEDICAL CENTER

PLEASE TAKE NOTICE that at 9:30 AM on November 30, 2006, at the Durham Marriott, 201 Foster Street, Durham, North Carolina 27701, or at such other date, time and place as the parties may mutually agree, defendant CAREFX CORPORATION ("Carefx") by its attorneys, will take the deposition of Duke University Medical Center.

In accordance with Rule 45, Fed. R. Civ. P., a subpoena will be served on Duke University Medical Center requesting it to produce the documents and things identified in the attached Schedule A, and requesting it to designate one or more officers, directors, or managing agents, or other persons who consent to testify on Duke University Medical Center's behalf as to subject matters set forth in the attached Schedule B.

The deposition will be recorded by stenographic and/or videographic means before an officer authorized to administer oaths by the laws of the United States. The deposition will continue from day to day until completed.

You are invited to attend.

POTTER ANDERSON & CORROON LLP

OF COUNSEL:

John W. Osborne
Peter N. Fill
Morgan & Finnegan, L.L.P.
3 World Financial Center
New York, NY 10281
Tel: (212) 415-8700

Dated: October 30, 2006
758508 / 30132

By: */s/ Kenneth L. Dorsney*
Richard L. Horwitz (#2246)
Kenneth L. Dorsney (#3726)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, Delaware 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
kdorsney@potteranderson.com

Attorneys for Defendant Carefx Corp.

UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF NORTH CAROLINA

SENTILLION, INC., Plaintiff and Counterclaim-Defendant, v. CAREFX CORP., Defendant and Counterclaim-Plaintiff.	SUBPOENA IN A CIVIL CASE CASE NO. Civil Action No. 06-013 (SLR) (pending in the United States District Court for the District of Delaware)

To:

Duke University Medical Center
2400 Pratt Street
Suite 4000
Durham, NC
(919) 684-8111

☐ YOU ARE COMMANDED to appear in the United States District Court at the place, date and time specified below to testify in the above case.

PLACE OF TESTIMONY	COURTROOM / DATE AND TIME

☒ YOU ARE COMMANDED to appear at the place, date and time specified below to testify at the taking of a deposition in the above case.

See attached Schedule B.

PLACE OF TESTIMONY	DATE AND TIME
Durham Marriott 201 Foster Street Durham, North Carolina 27701	November 30, 2006 9:30 A.M.

☒ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date and time specified below (list documents or objects).

See attached Schedule A.

PLACE	DATE AND TIME
Harris Investigative Services 145 Scotts Pine Circle Wake Forest, NC 27587-5484 (919) 451-8818	November 22, 2006 9:30 A.M.

☐ YOU ARE COMMANDED to produce and permit inspection of the following premises at the date and time specified below.

PREMISES	DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rule of Civil Procedure 30(b)(6).

ISSUING OFFICER SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)	DATE
Attorney for Defendant Carefx Corp.	October 30, 2006

ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER

Richard L. Horwitz

Hercules Plaza, 6th Floor, 1313 N. Market Street

Wilmington, Delaware 19899-0951 Tel: (302) 984-6000

PROOF OF SERVICE

SERVED	DATE	PLACE
SERVED ON (PRINT NAME)		MANNER OF SERVICE
SERVED BY (PRINT NAME)		TITLE

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Proof of Service is true and correct.

Executed on _____
DATE SIGNATURE OF SERVER

_____
ADDRESS OF SERVER

RULE 45. FEDERAL RULES OF CIVIL PROCEDURE, PARTS C & D:

(c) PROTECTION OF PERSONS SUBJECT TO SUBPOENAS.

(1) A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The court on behalf of which the subpoena was issued shall enforce this duty and impose upon the party or attorney in breach of this duty an appropriate sanction, which may include, but is not limited to, lost earnings and a reasonable attorney's fee.

(2) (A) A person commanded to produce and permit inspection and copying of designated books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(2) (B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection and copying may, within 14 days after service of subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to inspection or copying of any or all of the designated materials or of the premises. If objection is made, the party serving the subpoena shall not be entitled to inspect and copy the materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel production. Such an order to compel production shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded.

(3) (A) On timely, motion, the court by which a subpoena was issued shall quash or modify the subpoena if it:

(i) fails to allow reasonable time for compliance;

(ii) requires a person who is not a party or an officer of a party to travel to a place more than 100 miles from the place where that person resides, is employed or regularly transacts business in person, except that, subject to the provisions of clause (C)(3)(B)(iii) of this rule, such a person may in order to attend trial be commanded to travel from any such place within the state in which the trial is held, or

(iii) requires disclosure of privileged or other protected matter and no exception or waiver applies, or

(iv) subjects a person to undue burden.

(3) (B) If a subpoena

(i) requires disclosure of a trade secret or other confidential research, development, or commercial information, or

(ii) requires disclosure of an unretained expert's opinion or information not describing specific events or occurrences in dispute and resulting from the expert's study made not at the request of any party, or

(iii) requires a person who is not a party or an officer of a party to incur substantial expense to travel more than 100 miles to attend trial, the court may, to protect a person subject to or affected by the subpoena, quash or modify the subpoena or, if the party in whose behalf the subpoena is issued shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated, the court may order appearance or production only upon specified conditions.

(d) DUTIES IN RESPONDING TO SUBPOENA.

(1) A person responding to a subpoena to produce documents shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the demand.

(2) When information subject to a subpoena is withheld on a claim that it is privileged or subject to protection as trial preparation materials, the claim shall be made expressly and shall be supported by a description of the nature of the documents, communications, or things not produced that is sufficient to enable the demanding party to contest the claim.

SCHEDULE A

INSTRUCTIONS

1. This Request is intended to include all documents and things in the possession, custody or control of Duke University Medical Center and/or any representative of Duke University Medical Center, wherever located.

2. Such documents and things shall be produced as they are kept in the usual course of business, or they shall be organized by Duke University Medical Center to correspond to the categories in this request, in accordance with Fed. R. Civ. P. 34(b).

3. Each Request is to be fully and separately answered. Should an objection to a Request be interposed, it should indicate the part of the Request to which it is directed.

4. With respect to each Request, if Duke University Medical Center is able to provide some, but not all, of the information requested, it must provide such information as it is able, and identify specifically the items or aspects as to which it does not have sufficient information to respond fully.

5. To the extent any of the following Requests may include language quoted from the Complaint, Answer, Counterclaims, '313 patent, '556 patent or any other document, this in no way constitutes an admission of any factual allegation or concession of any legal proposition contained therein.

6. Unless otherwise noted, these Requests are not limited in time.

7. If any document or thing covered by these Requests is withheld pursuant to a claim of privilege, pursuant to the Federal Rules of Civil Procedure, Duke University

Medical Center shall state the grounds for such refusal including any claim of privilege(s) or any other claim of immunity from disclosure in sufficient detail to permit the Court to adjudicate the validity of the refusal. In particular, Duke University Medical Center must provide a list, at the time documents and things are produced responsive to these Requests, which identifies each such document or thing for which any such privilege is claimed, together with the following information with respect to any such document or thing withheld: authors(s), sender(s), addressee(s), recipients(s), indicated copy or blind copy; date of original and date of handwritten or subsequent annotations, notes or routing notations; nature and general subject matter of document and any such annotation, notes, or notations; number of pages, and separately, the number of attached pages, nature and general subject matter of attachment(s); legal basis on which the privilege is claimed, whether the claimed privilege is waived as to any part; and the specific request to which the document or thing relates. Duke University Medical Center shall furnish the privileged document list in chronological order.

8. In the event that any document or thing called for by these Requests is destroyed, lost, discarded, or otherwise disposed of, such document or thing shall be identified as completely as possible, including, without limitation, the following information: date of disposal; manner of disposal; reason for disposal; person authorizing the disposal; and person disposing the document.

9. To the extent any Request is objected to as overly broad and/or unduly burdensome, set forth the factual basis for such claim, set forth the more narrowly-defined basis, if any, on which you are prepared or able to respond to such request, and respond to the Request on that basis.

10. To the extent that any Request is objected to as vague or ambiguous, identify the particular words, terms, or phrases that are asserted to make such Request vague or ambiguous, specify the meaning actually attributed by you to such words, terms, or phrases for purposes of your response to such Request, and respond to the Request accordingly.

11. If Duke University Medical Center knows of the existence, past or present, of any documents or things described or requested below, but is unable to produce such documents because they are not presently in the possession, custody or control of Duke University Medical Center, identify each such document or thing and the person who has possession, custody or control of such document or thing.

12. Pursuant to Rule 26(e)(2) of the Federal Rules of Civil Procedure, these Requests shall be deemed continuing so as to require supplemental production by Duke University Medical Center in the event it obtains or discovers additional documents between the time of initial production and the time of hearing or trial.

DEFINITIONS

In accordance with the Federal Rules of Civil Procedure, the following definitions shall apply to these document requests:

1. *Communication*. The term "communication" means the transmittal of information (in the form of facts, ideas, inquiries, or otherwise).

2. *Communications, Publications or Written Communications*. The terms "communications," "publications," or "written communications" as used in these Requests, refer to any communication or publication regardless of the manner in which

such communication or publication took place, including computer-generated communications such as E-mail, voice mail, etc.

3. *Conversations or Oral Communications*. "Conversations" or "oral communications" as used in these Requests, refers to any oral communications regardless of the manner in which such oral communication took place.

4. *Document*. The terms "document" or "documents," as used in these Requests is defined to be synonymous in meaning and equal in scope to the broadest usage of this term in Fed. R. Civ. P. 34(a) and includes, but is not limited to, all materials in Fed. R. Evid. 1001, and comprises any writing in the custody, possession or control of Duke University Medical Center or known to it -- whether printed, recorded, in computer data bases, computer memory or other storage media, reproduced by any process, or written or produced in hand, and whether or not claimed to be privileged or exempt from production for any reason -- including, but not limited to, letters, reports, agreements, communications, including intra-company communications, E-mails, correspondence, telegrams, memoranda, summaries or records of personal conversations, diaries, forecasts, photographs, audiotape, videotape, wire or other recordings, statistical statements, graphs, charts, plans drawings, minutes or records of meetings including directors' meetings, minutes or records of conferences, expressions or statements of policy, lists of persons attending meetings or conferences, reports and/or summaries of interviews, reports and/or summaries of investigations, opinions, or reports of consultants, brochures, pamphlets, advertisements, circulars, trade letters, press releases, drafts of any documents, revisions of drafts of any documents, invoices, receipts and original or preliminary notes. Any comments or notations appearing on any documents

and not a part of the original text, is to be considered a separate "document." A draft or non-identical copy is a separate "document" within the meaning of this term.

5. *Thing*. The term "thing" shall refer to any tangible object other than a document and includes objects of every kind and nature, including, but not limited to, samples, products, prototypes, models, specimens, slides, photographs, video tapes, audio tapes, computer disks, compact discs, or any other electronic medium by which information is stored or communicated.

6. *Identify (With Respect to Persons)*. When referring to a person, "to identify" means to give, to the extent known, the person's full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. Once a person has been identified in accordance with this subparagraph, only the name of that person need be listed in response to subsequent discovery requesting the identification of that person.

7. *Identify (With Respect to Documents)*. When referring to documents, "to identify" means to give, to the extent known, the

(a) type of document;

(b) general subject matter;

(c) date of the document; and

(d) author(s), addressee(s), distributee(s) and recipient(s).

8. *Parties*. The term "SENTILLION" shall refer to Plaintiff and Counterclaim Defendant SENTILLION, INC., and its officers, directors, employees, agents, representatives, partners, corporate parent, subsidiaries, predecessors, attorneys

and affiliates and all other individuals and/or entities acting on its behalf and any other entity or person over which any of the foregoing may exercise control.

The term "CAREFX" shall refer to Defendant and Counterclaim Plaintiff CAREFX CORPORATION, its officers, directors, employees, agents, representatives, partners, corporate parent, affiliates, predecessors, attorneys, subsidiaries, and all other individuals and/or entities acting on its behalf and any other entity or person over which any of the foregoing may exercise control.

9. *Person.* The term "person" is defined as any natural person or any business, legal, or governmental entity or association.

10. *Concerning.* The term "concerning" means referring to, describing, evidencing, or constituting.

11. *Third Parties.* The term "third parties" refers to individuals or entities that are not parties to this action.

12. *Referring or Relating.* The terms "referring" and "relating" shall be construed in the broadest sense to mean (1) information which contains or comprises any communication (including representations, requests, demands, and the like) referred to in these requests, or (2) information which discusses, mentions or refers, whether directly or indirectly, to the subject matter of the request.

13. *'313 Patent.* The term "'313 patent" means U.S. Patent No. 6,941,313 to Seliger et al. and all related U.S. patents and patent applications including, but not limited to, all patents and patent applications, whether issued, abandoned, or pending, claiming priority to U.S. application Serial Nos. 10/014,341 and/or 60/254,753. A copy of U.S. Patent No. 6,941,313 is attached as Exhibit 1.

14. *'556 Patent.* The term "'556 patent" means U.S. Patent No. 6,993,556 to Seliger et al. and all related U.S. patents and patent applications including, but not limited to, all patents and patent applications, whether issued, abandoned or pending, claiming priority to U.S. application Serial Nos. 09/545,396; 60/128,145; 60/135,907; 60/136,670; 60/139,235; 60/139,145; 60/146,722 and/or 60/145,681. A copy of U.S. Patent Number 6,993,556 is attached as Exhibit 2.

15. *Prior Art* The term "prior art" encompasses by way of example, and without limitation, the subject matter described in each and every subparagraph of 35 U.S.C. §§ 102 and 103.

16. *Healthcare Information.* The term "healthcare information" means any and all information associated with, resulting from, related to, or involved with the healthcare industry or rendition of healthcare services.

17. *CCOW.* The term "CCOW" or "Clinical Context Object Workgroup" refers to the organization and/or standard related to healthcare context management and any and all associates, affiliates, predecessors, successors, variations, versions or drafts of such organization and/or standard.

18. The singular shall include the plural and vice versa. The terms "and" and "or" shall be both conjunctive and disjunctive.

REQUESTS FOR PRODUCTION OF DOCUMENTS AND THINGS

REQUEST NO. 1

All documents and things referring to, relating to or concerning the development of the CCOW standard.

REQUEST NO. 2

All documents and things referring to, relating to or concerning the development of a CCOW enabled context manager prior to December 11, 2001.

REQUEST NO. 3

All documents and things referring to, relating to, or concerning any work performed at Duke University Medical Center or on behalf of Duke University Medical Center with regard to the development of the CCOW standard, including all versions thereof, or its predecessor(s) or any other standard or protocol involving context management in healthcare information systems including, but not limited to, all such work performed, directed by, or participated in by W. Edward Hammond.

REQUEST NO. 4

All documents and things referring to, relating to, or concerning the development and or activities of the Visual Integration Research Center.

REQUEST NO. 5

All documents and things that may be considered prior art to the '313 patent or the '556 patent.

REQUEST NO. 6

All documents and things referring to, relating to or concerning Robert Seliger, David Fusari and/or Elaine Seliger.

REQUEST NO. 7

All documents and things referring to, relating to or concerning SENTILLION.

REQUEST NO. 8

All documents and things referring to, relating to or concerning the validity of the '313 patent and the '556 patent under 35 U.S.C. § 102.

REQUEST NO. 9

All documents and things referring to, relating to or concerning the validity of the '313 patent and the '556 patent under 35 U.S.C. § 103.

REQUEST NO. 10

All documents and things referring to, relating to or concerning the validity of the '313 patent and the '556 patent under 35 U.S.C. § 112.

REQUEST NO. 11

All documents and things referring to, relating to or concerning the state of the art of the subject matter of the '313 patent and the '556 patent as of December 11, 2000 and April 7, 1999 respectively.

REQUEST NO. 12

All documents and things referring to, relating to, or concerning any communications between Duke University Medical Center and any person relating to the '313 and or the '556 patents and applications from which the patent(s) claim priority.

EXHIBIT 1

US006941313B2

(12) **United States Patent**
Seliger et al.

(10) **Patent No.: US 6,941,313 B2**
(45) **Date of Patent: Sep. 6, 2005**

(54) **CONTEXT MANAGEMENT WITH AUDIT CAPABILITY**

(75) Inventors: **Robert Seliger**, Winchester, MA (US); **David Fusari**, Groton, MA (US)

(73) Assignee: **Sentillion, Inc.**, Andover, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 584 days.

(21) Appl. No : **10/014,341**

(22) Filed: **Dec. 11, 2001**

(65) **Prior Publication Data**

US 2002/0107875 A1 Aug. 8, 2002

Related U.S. Application Data

(60) Provisional application No. 60/254,753, filed on Dec. 11, 2000.

(51) **Int. Cl.**[7] **G06F 17/30**

(52) **U.S. Cl.** ..... **707/101**; 707/1; 707/104.1; 707/103 R; 705/3; 717/108; 717/101

(58) **Field of Search** ..... 707/1, 104.1, 101, 707/103 R–103 Z, 209, 203, 8; 717/100, 101, 108; 705/2, 3

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,524,238 A	*	6/1996	Miller et al.	707/4
5,566,319 A		10/1996	Lenz	711/147
5,878,258 A	*	3/1999	Pizi et al.	719/320
6,134,552 A	*	10/2000	Fritz et al.	707/10
6,397,253 B1	*	5/2002	Quinlan et al.	709/227
6,401,138 B1	*	6/2002	Judge et al.	719/328
6,560,655 B1	*	5/2003	Grambihler et al.	709/248
6,691,118 B1	*	2/2004	Gongwer et al.	707/100

OTHER PUBLICATIONS

"Architecture for a Distributed Computing Environment Test Application—Harmonic," IBM Technical Disclosure Bulletin, IBM Corp., New York, NY, vol. 39, No. 6, Jun. 1, 1996, pp. 259–261.

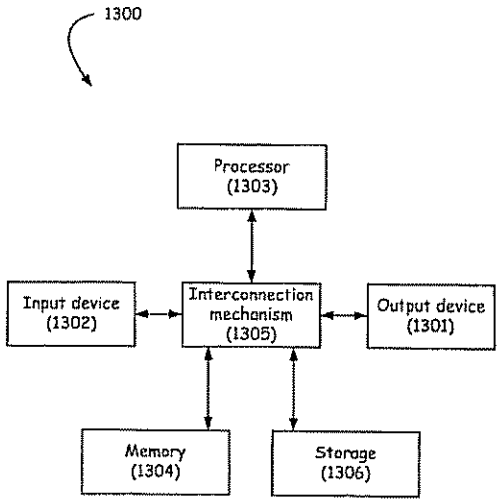
* cited by examiner

Primary Examiner—Greta Robinson
Assistant Examiner—Cheryl Lewis
(74) *Attorney, Agent, or Firm*—Wolf, Greenfield & Sacks, P.C.

(57) **ABSTRACT**

A context management framework is given that provides in various embodiments, numerous advantages over previously-existing systems. In some instances, an architecture having a centralized storage location coupled to a context manager is provided for servicing and logging context events from a plurality of sources. This type of system uses a synchronization scheme to perform orderly storage and retrieval of data to and from the centralized storage location. In other instances, information stored in the centralized storage location or signals from the context manager are used to achieve an auditing capability for reviewing and acting on context data events and gestures. Selective blocking or allowance of impending context gestures or data-access events is accomplished based on a rule set or lookup table containing rules or other data to make such access-control decisions. Access to private data and other security measures may thus be implemented using the teachings presented herein. Furthermore, a communication paradigm, using a Web-proxy, which identifies ordinarily-unidentified applications to a context manager is provided according to some embodiments of the invention.

39 Claims, 16 Drawing Sheets



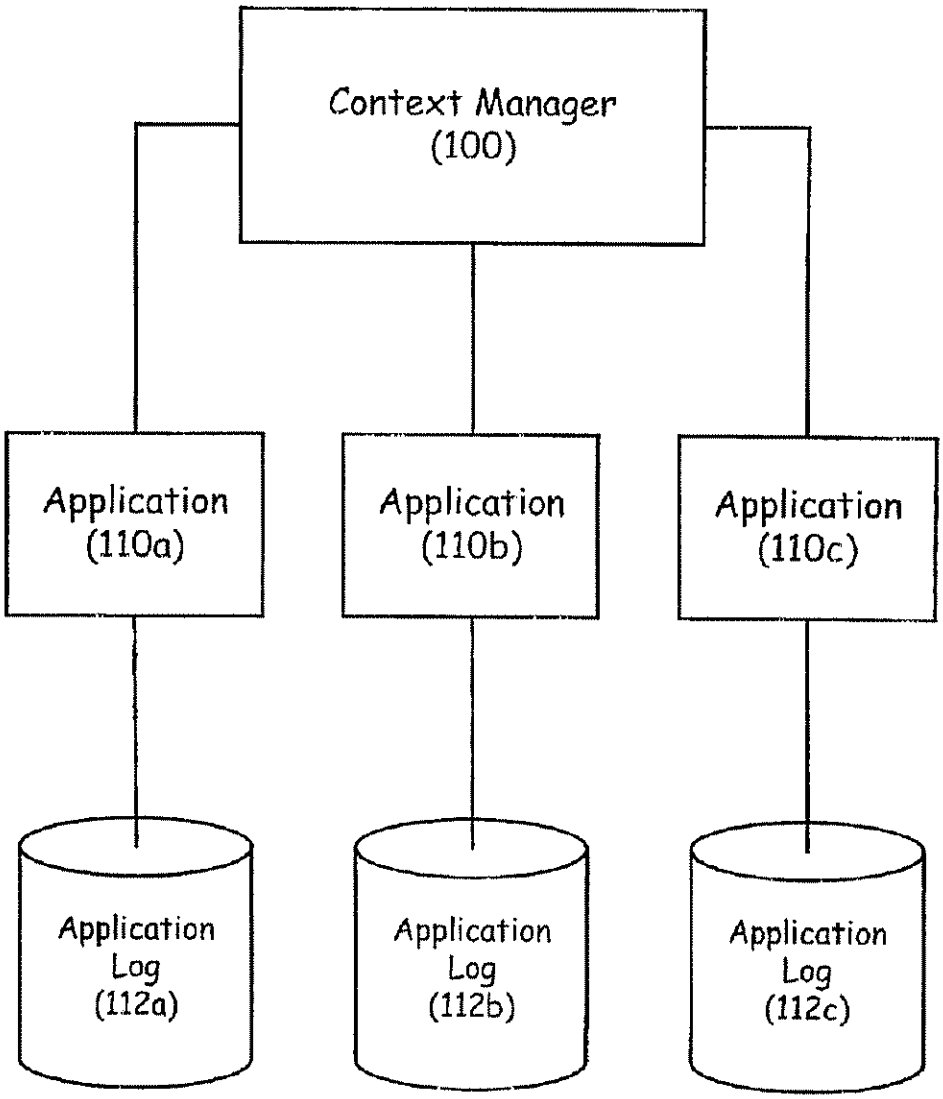


FIG. 1
(PRIOR ART)

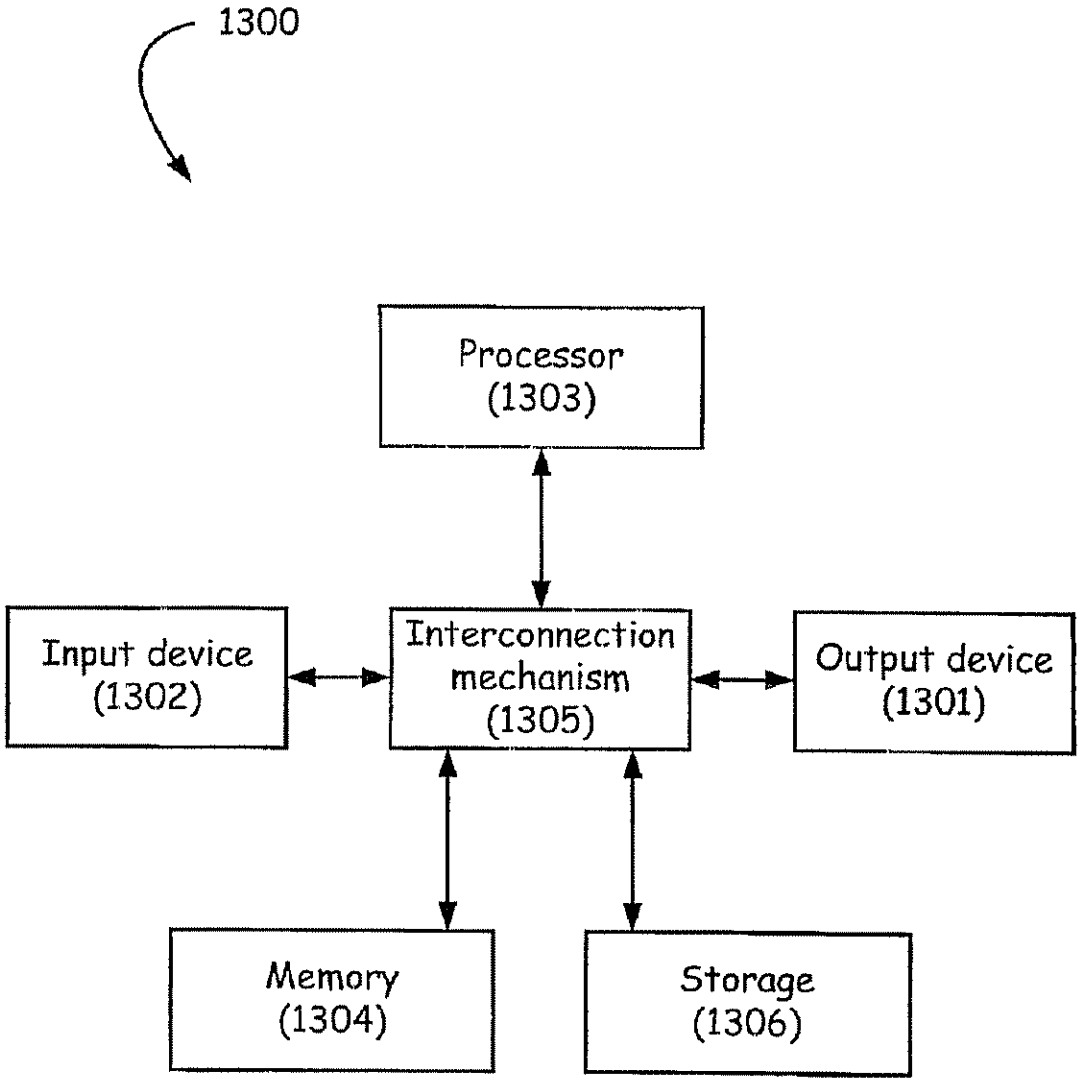

1300
Processor
(1303)
Input device
(1302)
Interconnection
mechanism
(1305)
Output device
(1301)
Memory
(1304)
Storage
(1306)

FIG. 2

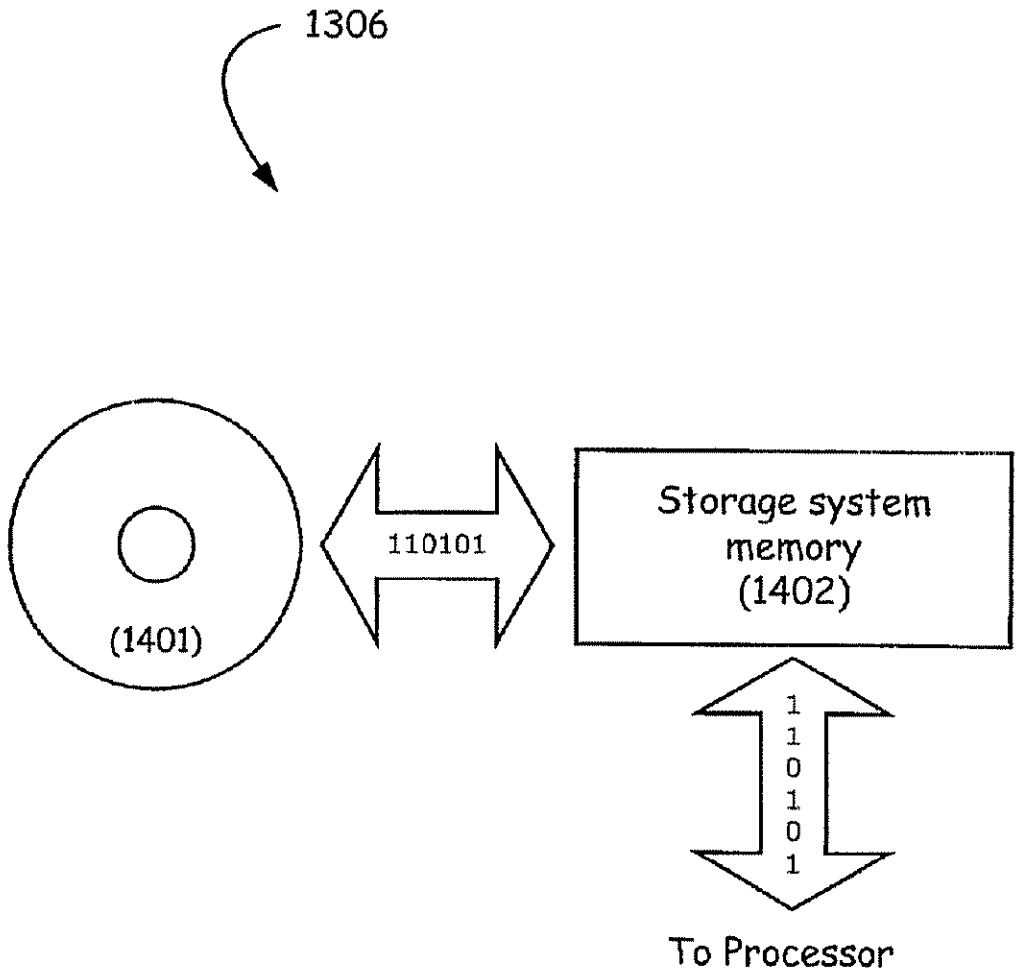

1306
(1401)
110101
Storage system memory (1402)
1 1 0 1 0 1
To Processor

FIG. 3

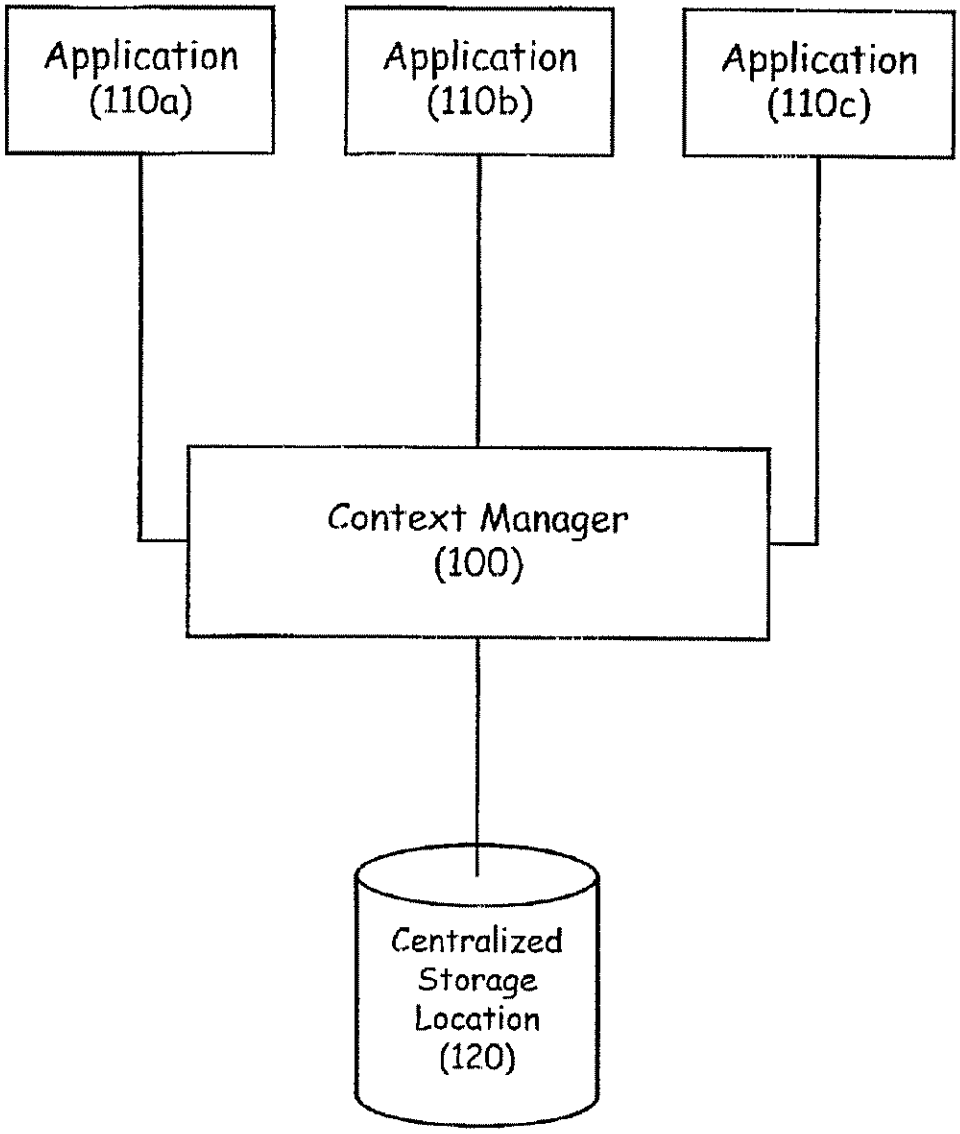

Application (110a)
Application (110b)
Application (110c)
Context Manager (100)
Centralized Storage Location (120)

FIG. 4

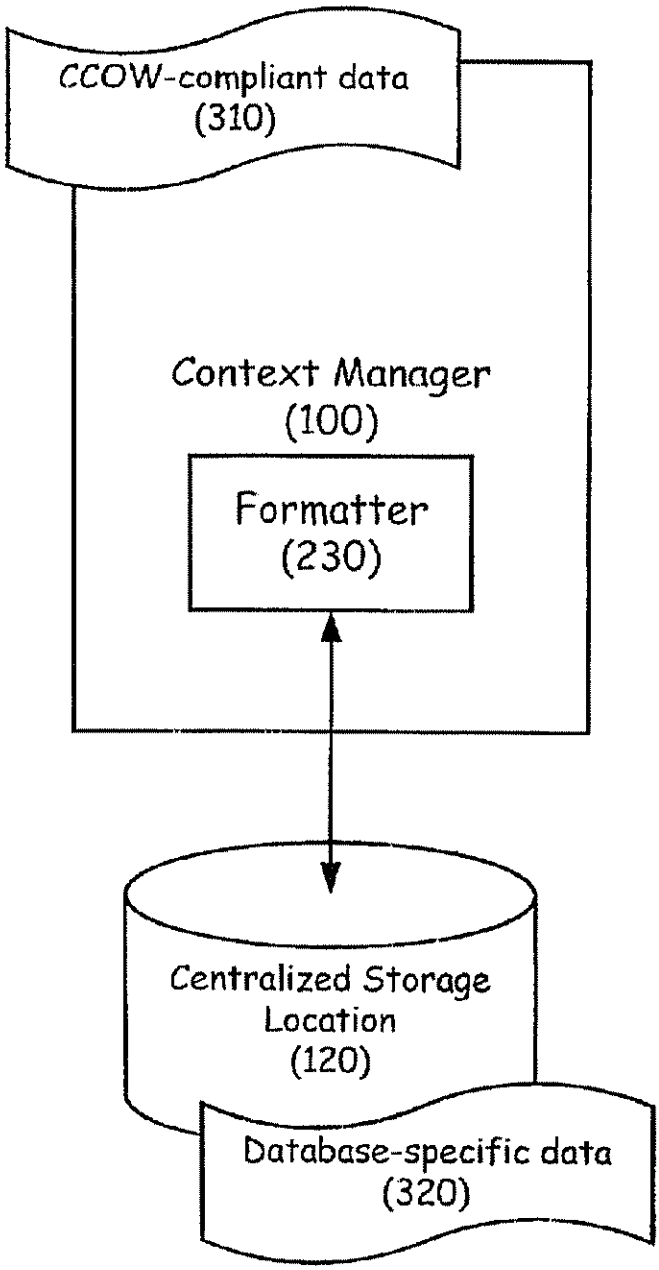

CCOW-compliant data
(310)
Context Manager
(100)
Formatter
(230)
Centralized Storage
Location
(120)
Database-specific data
(320)

FIG. 5

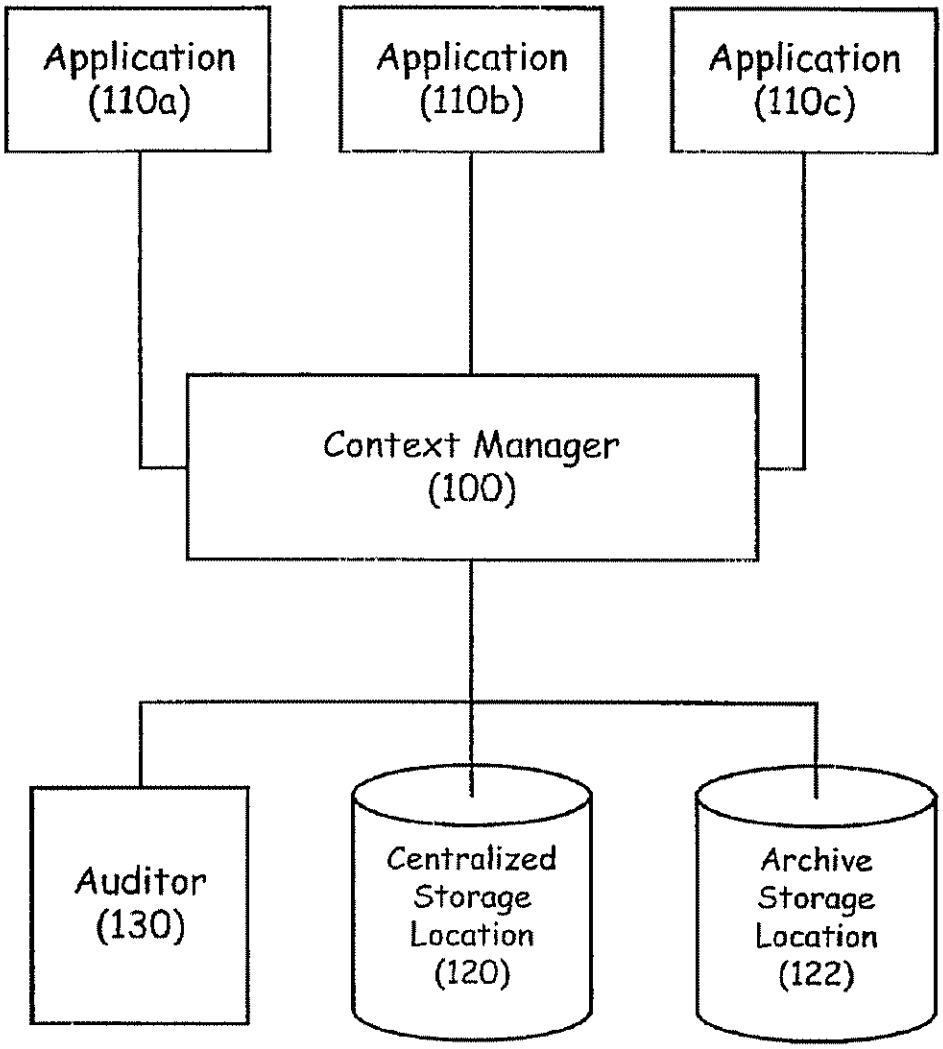

Application (110a)
Application (110b)
Application (110c)
Context Manager (100)
Auditor (130)
Centralized Storage Location (120)
Archive Storage Location (122)

FIG. 6

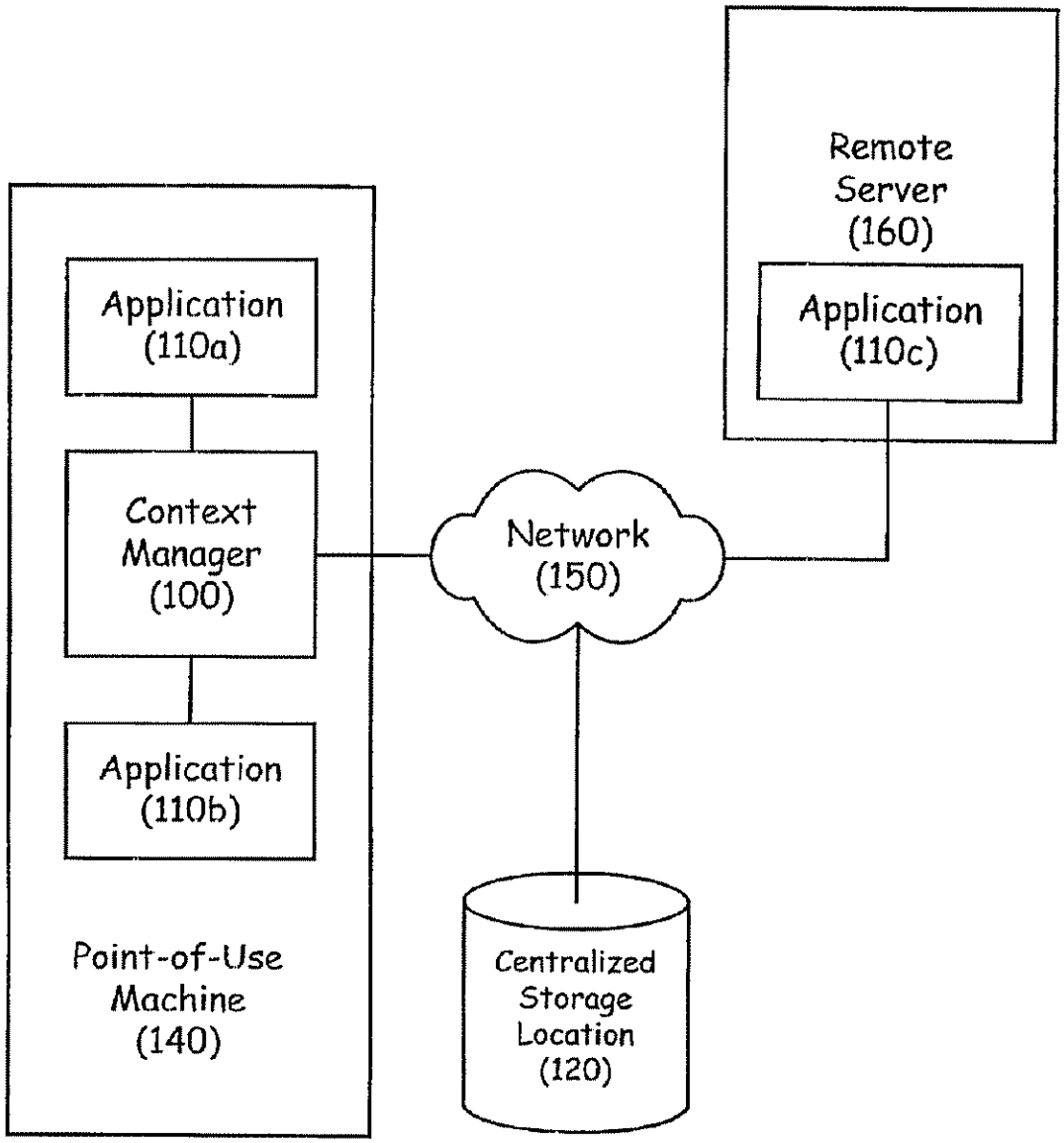

Remote
Server
(160)
Application
(110c)
Application
(110a)
Context
Manager
(100)
Network
(150)
Application
(110b)
Point-of-Use
Machine
(140)
Centralized
Storage
Location
(120)

FIG. 7

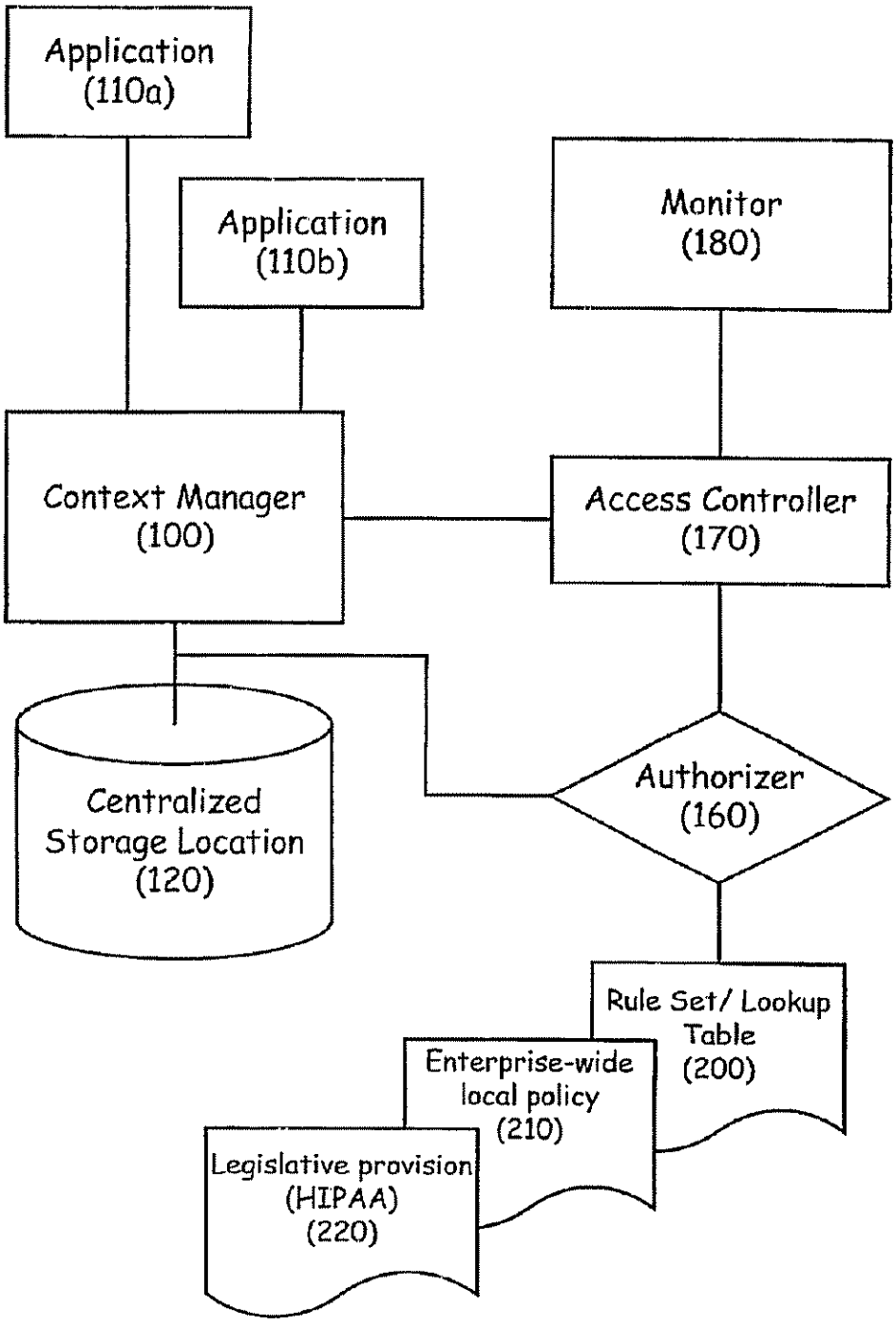

Application (110a)
Application (110b)
Monitor (180)
Context Manager (100)
Access Controller (170)
Centralized Storage Location (120)
Authorizer (160)
Rule Set/ Lookup Table (200)
Enterprise-wide local policy (210)
Legislative provision (HIPAA) (220)

FIG. 8

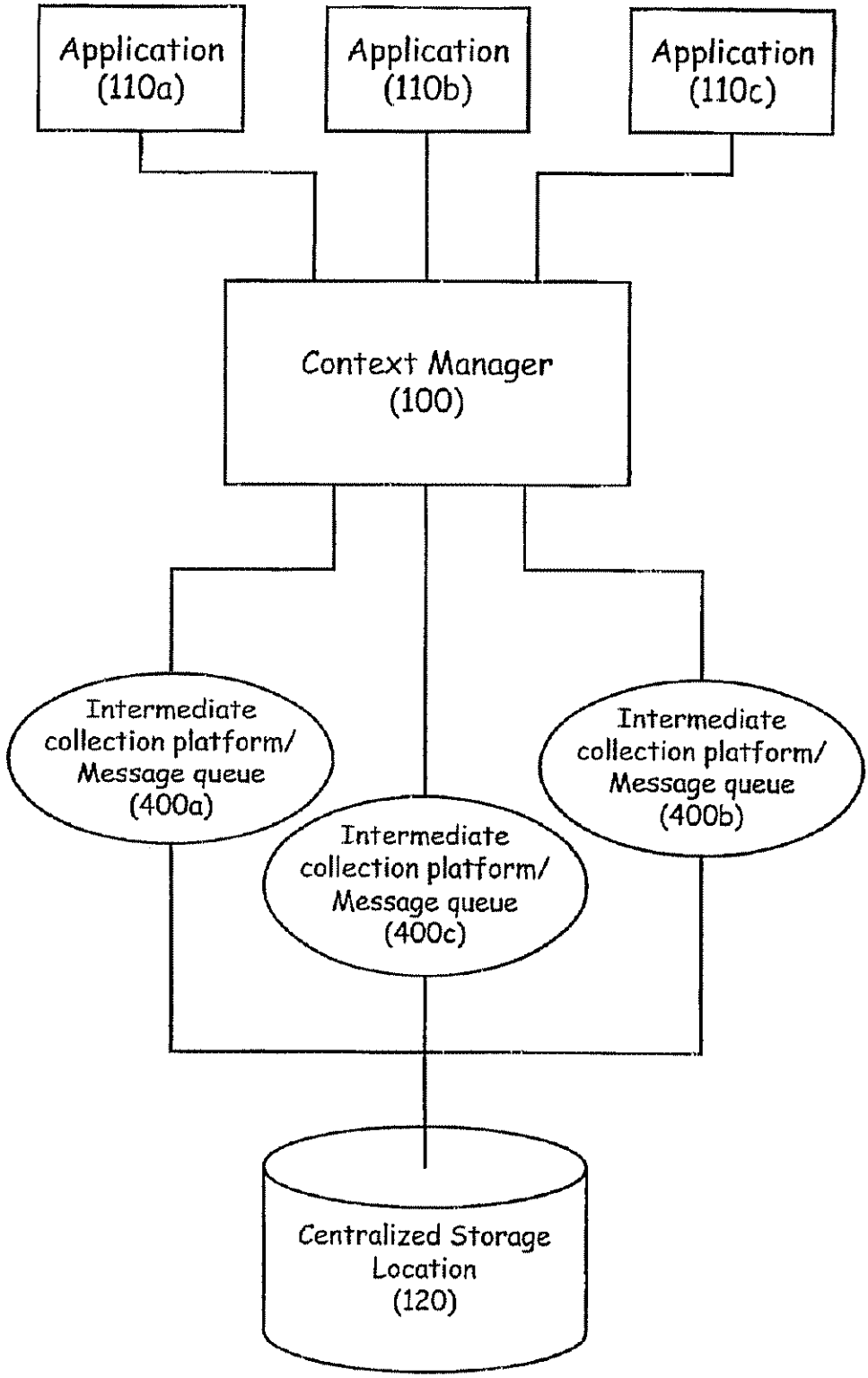

Application (110a)
Application (110b)
Application (110c)
Context Manager (100)
Intermediate collection platform/ Message queue (400a)
Intermediate collection platform/ Message queue (400c)
Intermediate collection platform/ Message queue (400b)
Centralized Storage Location (120)

FIG. 9

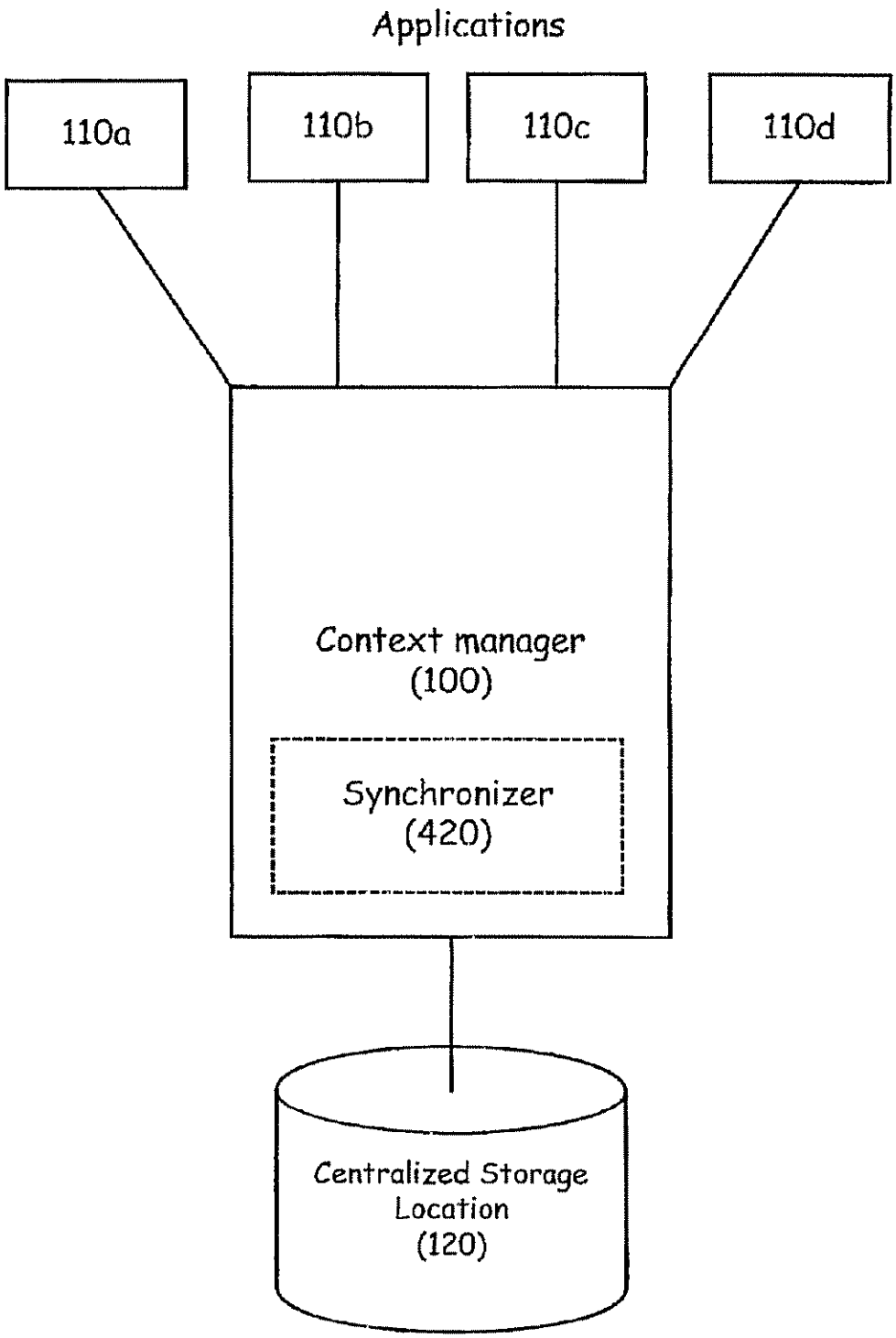

Applications
110a
110b
110c
110d
Context manager
(100)
Synchronizer
(420)
Centralized Storage
Location
(120)

FIG. 10

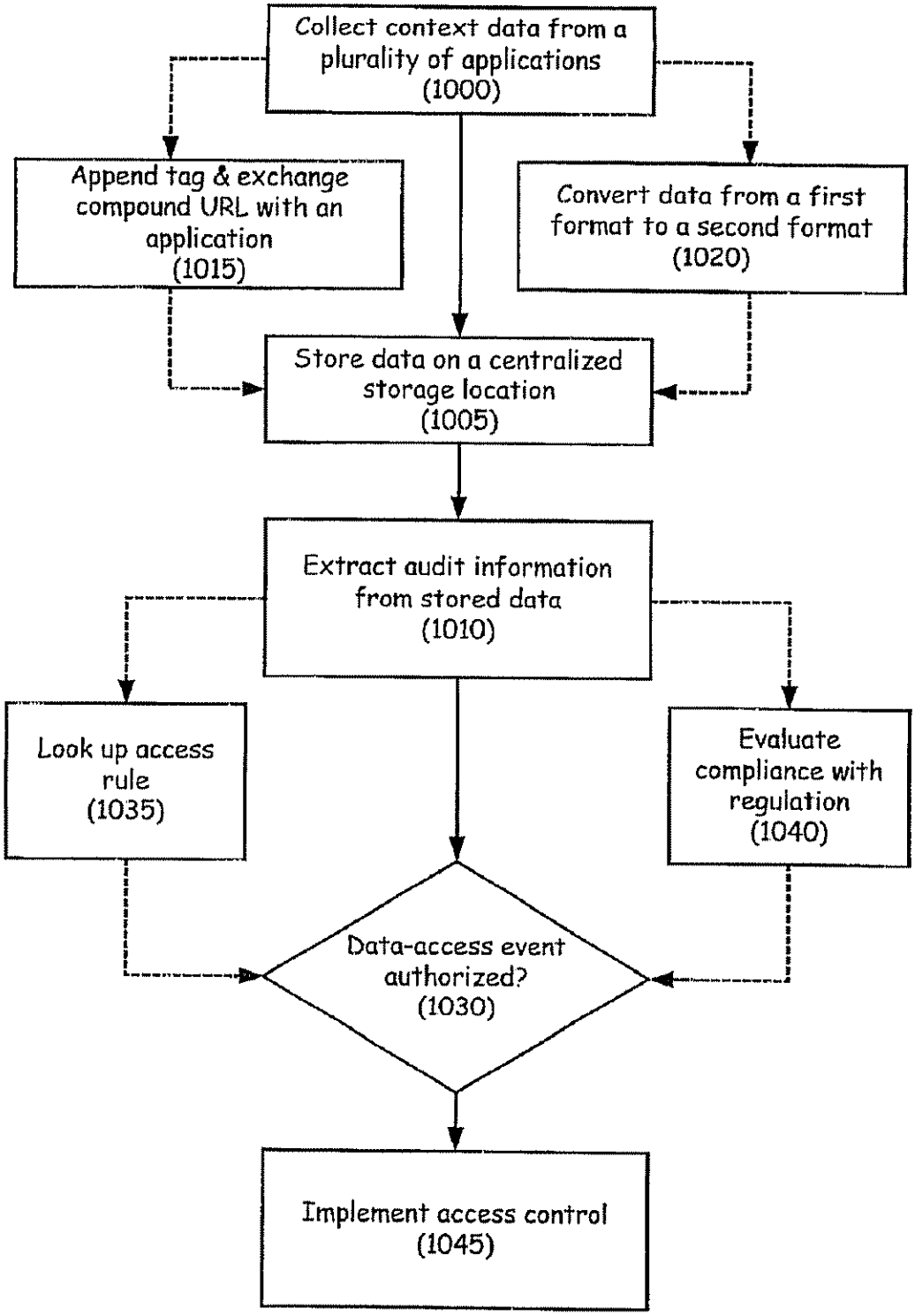

Collect context data from a plurality of applications (1000)
Append tag & exchange compound URL with an application (1015)
Convert data from a first format to a second format (1020)
Store data on a centralized storage location (1005)
Extract audit information from stored data (1010)
Look up access rule (1035)
Evaluate compliance with regulation (1040)
Data-access event authorized? (1030)
Implement access control (1045)

FIG. 11

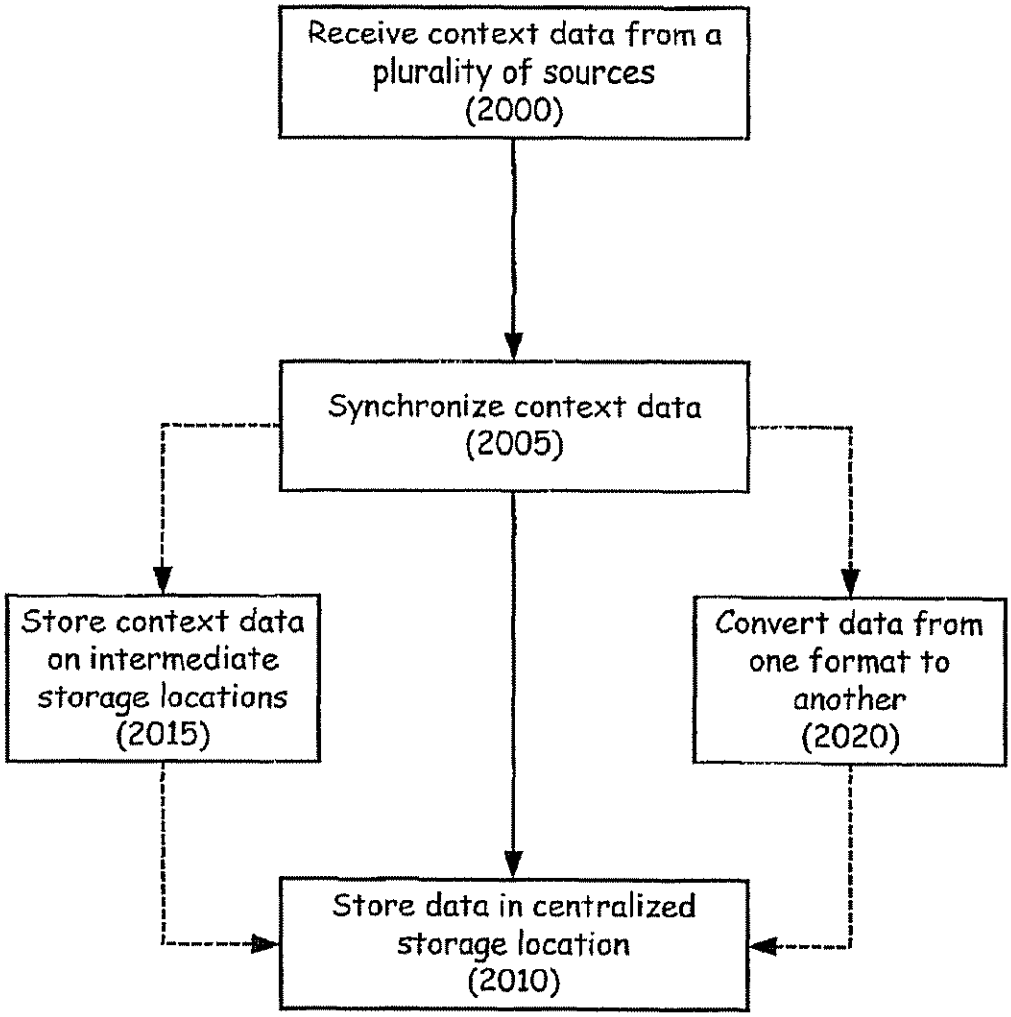

Receive context data from a plurality of sources (2000)
Synchronize context data (2005)
Store context data on intermediate storage locations (2015)
Convert data from one format to another (2020)
Store data in centralized storage location (2010)

FIG. 12

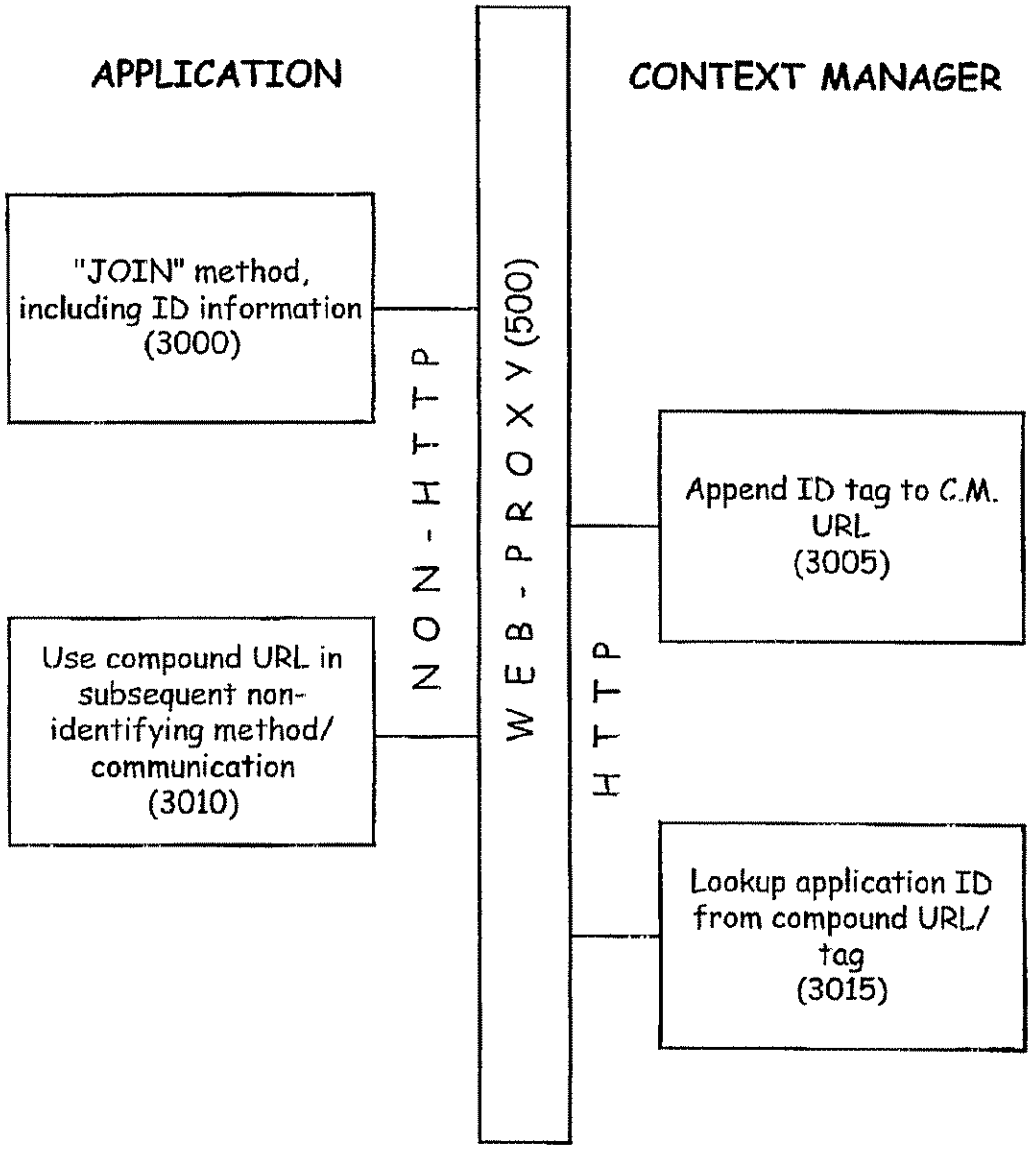

APPLICATION
CONTEXT MANAGER
"JOIN" method, including ID information (3000)
Use compound URL in subsequent non-identifying method/ communication (3010)
NON-HTTP
WEB-PROXY (500)
HTTP
Append ID tag to C.M. URL (3005)
Lookup application ID from compound URL/ tag (3015)

FIG. 13

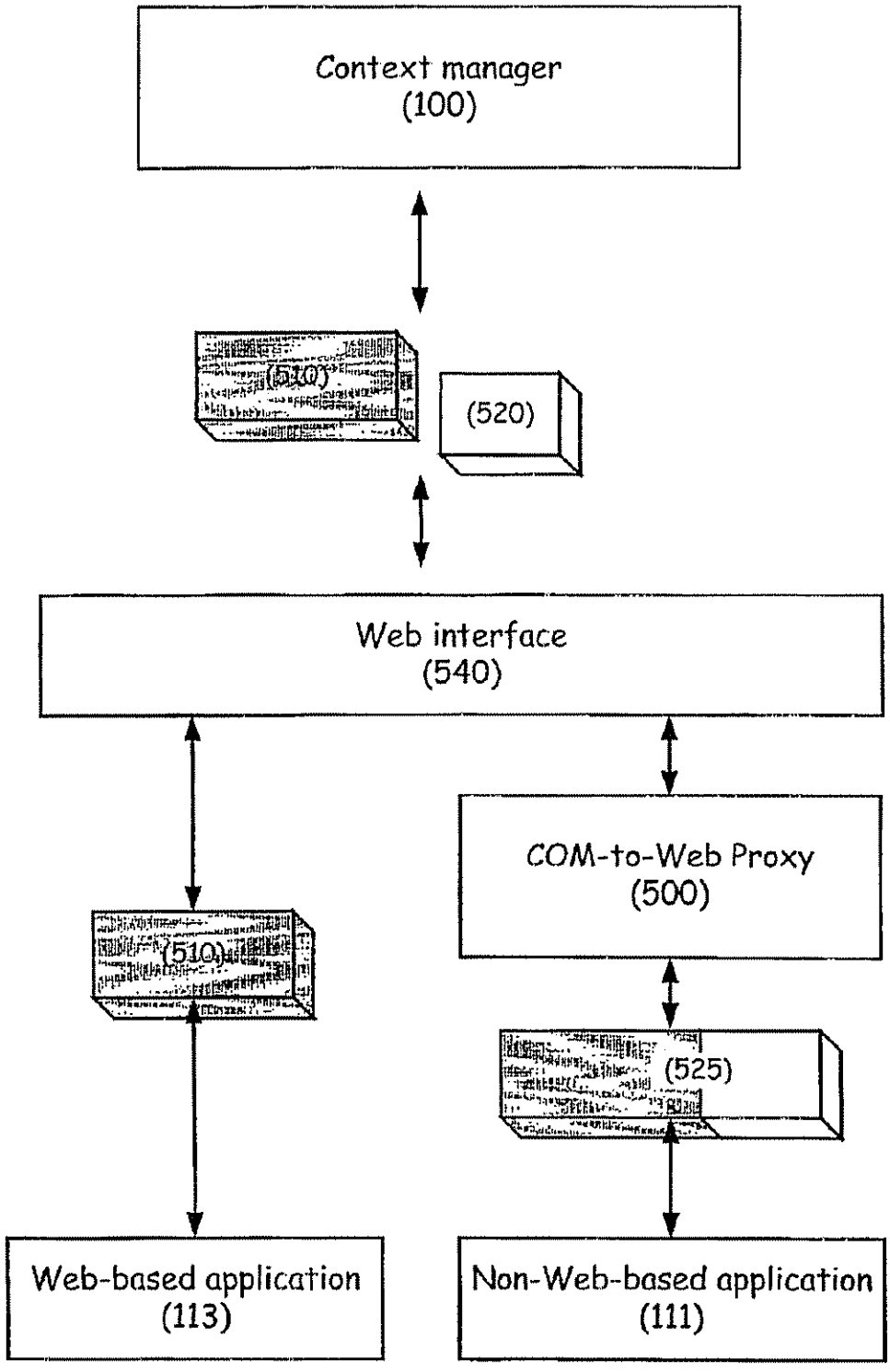

Context manager
(100)
(510)
(520)
Web interface
(540)
COM-to-Web Proxy
(500)
(510)
(525)
Web-based application
(113)
Non-Web-based application
(111)

FIG. 14

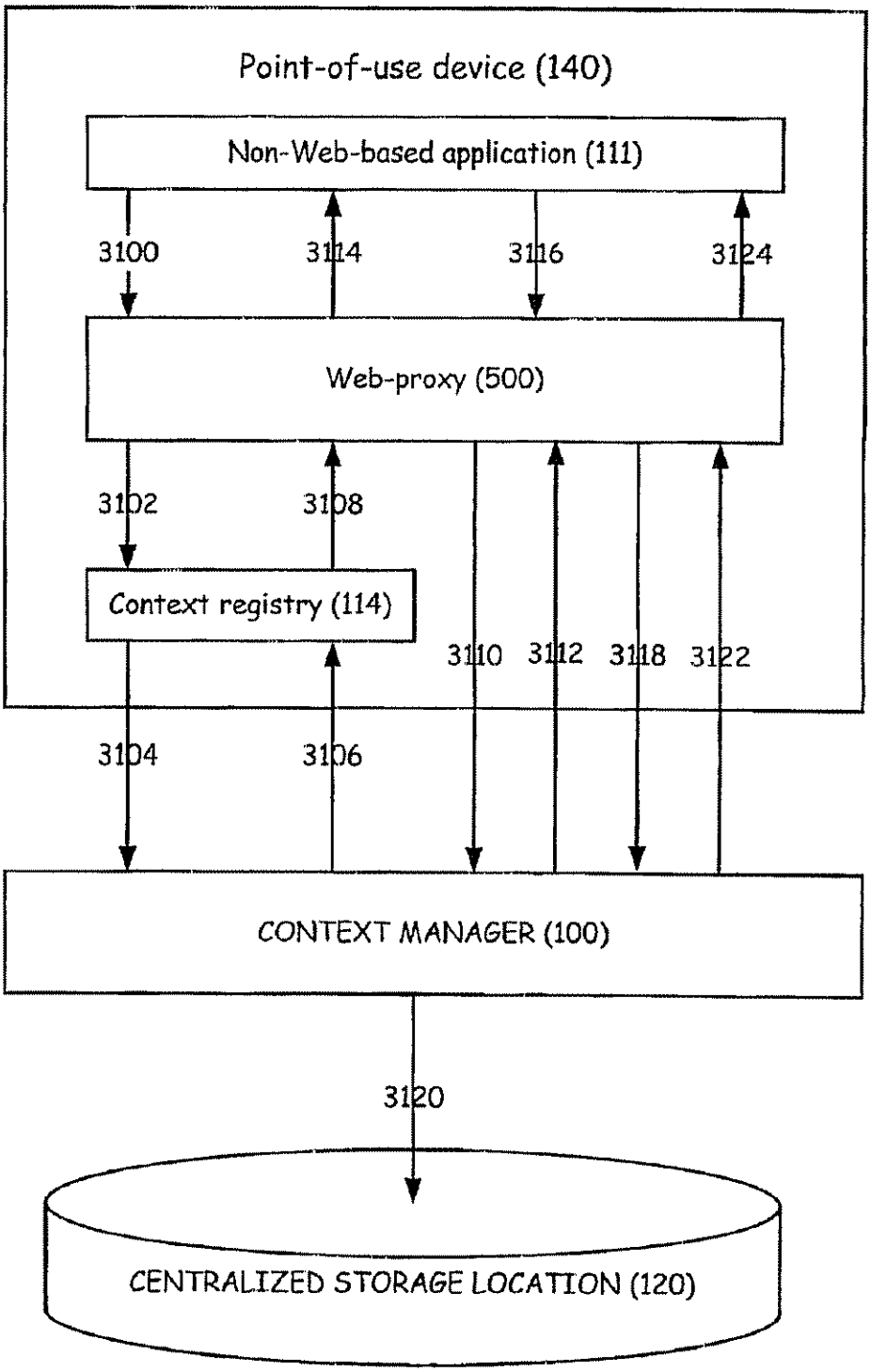

Point-of-use device (140)
Non-Web-based application (111)
3100
3114
3116
3124
Web-proxy (500)
3102
3108
Context registry (114)
3110
3112
3118
3122
3104
3106
CONTEXT MANAGER (100)
3120
CENTRALIZED STORAGE LOCATION (120)

FIG. 15

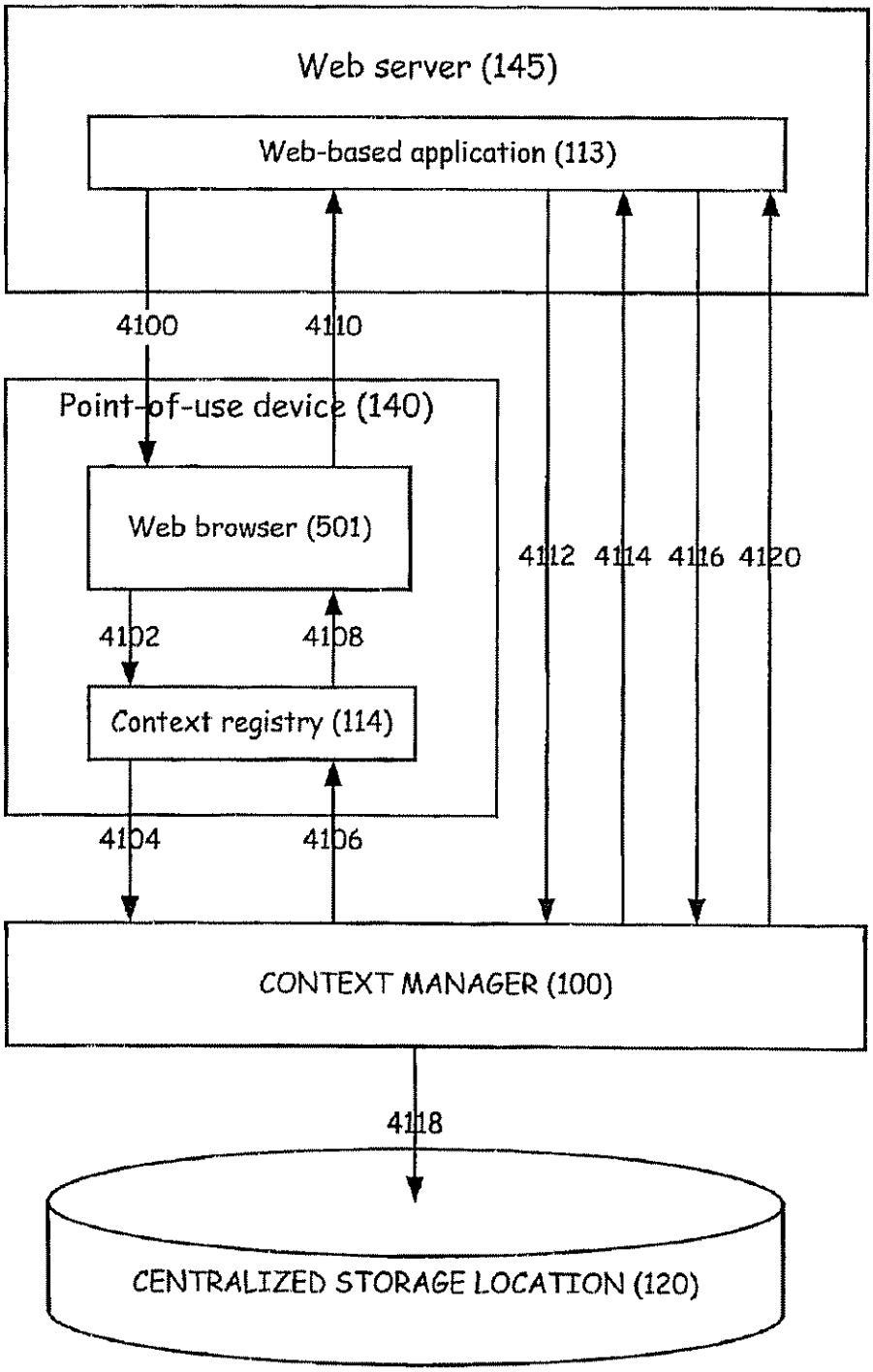

Web server (145)
Web-based application (113)
4100
4110
Point-of-use device (140)
Web browser (501)
4112
4114
4116
4120
4102
4108
Context registry (114)
4104
4106
CONTEXT MANAGER (100)
4118
CENTRALIZED STORAGE LOCATION (120)

FIG. 16

CONTEXT MANAGEMENT WITH AUDIT CAPABILITY

REFERENCE TO RELATED APPLICATION

This application claims the benefit of U S. Provisional Application Ser. No 60/254,753, filed Dec. 11, 2000, entitled SECURE AUDIT OF USER CONTEXT, which application is hereby incorporated herein by reference

TECHNICAL FIELD

The present disclosure relates generally to data processing systems, and more specifically to context management systems Yet more specifically, the disclosure relates to context management using a centralized storage location servicing a plurality of applications Auditing and control of information in a context management setting is also addressed

BACKGROUND

Context management, sometimes called visual integration, provides a framework, which operates, in conjunction with context-enabled software applications, to streamline and simplify and coordinate the process of accessing stored data and records responsive to actions by a user of the system If a common attribute is shared between data records to be accessed by the applications, this common attribute, such as log-in information, may need to be repetitively entered into the respective interfaces presented by each application Since the applications may not come from a single vendor, each application may further have a different interface or may require a different entry by an application user before the application retrieves and presents the data record which the user has asked for

Many fields of endeavor can benefit from the use of context management A brief list includes healthcare, sales, government administration, education, and insurance. An attempt has been made in certain industries, for example in the health care industry, to formulate a standard for exchange of context-related information between context-enabled applications The healthcare industry has developed an industry standard for context management, known as the Health Level Seven (HL7) CCOW standard, having roots in the once-active Clinical Context Object Workgroup Various versions, beginning with CCOW version 1 0, up to CCOW version 1 4, which is expected to be issued in early 2002, are available Other later versions can be expected to issue Each version of the CCOW standard incorporates some features of the previous versions of the standard, and the collection of features that generally describe these versions is hereinafter denoted by the "CCOW standard set" of features

In a clinical healthcare delivery setting, one application might be directed to patient billing records, and is primarily used by administrators and accountants, while another application that may run on the same platform could present medical image data, for use by physicians and medical professionals In such cases, a user, for example a patient's primary caregiver, may wish to first view medical record data or medical images for a particular patient, and in the same session view that patient's billing account information or insurance information Without context management, the primary caregiver would be required to enter data to identify him or herself in order to log in to the various databases containing the desired information, as well as provide patient identifying information so that the particular patient's records may be pulled up in the query If several such applications are open, it becomes time-consuming and

cumbersome to enter the required information and login data into each application's individual user interface Furthermore, mistakes in typing account numbers or social security numbers, etc , can occur more often when repetitive entry is required

In order to assist users who are using context-enabled applications, a "context manager" which supports context-enabled applications, is used to pass context data between one application and another "Context data" is information indicative of a condition or identity associated with users, applications, stored records, or any other information that facilitates or enables performance of inter-application or inter-platform functionality in a context management environment The context data may contain data useful for accessing data relating to or identifying an attribute of a user, machine, application, customer, or patient

By carrying out certain actions, referred to as "context gestures," a user using a context-managed environment causes context data to be generated and transmitted through the context manager The context gestures may take any of numerous forms, but generally are responsive to a need by the user to move between applications or windows executing in a data processing system The context in which the gestures are carried out may be transmitted from a first application to a second application to simplify the work of the user, as described above, so that the second applications "knows" what context the user is working in at the time the user shifts from using the first to using the second application This looking-ahead functionality is a shortcut that shifts some of the burden of cross-application work from the user to the context manager

A typical implementation of a context management system according to the prior art is shown in FIG 1 A context manager **100** is coupled to a plurality of context-enabled applications **110** Sometimes, a log **112** of activity associated with a particular application **110** is maintained by the applications **110** Since the logging capability is conventionally provided by the vendor of the particular application, e g **110***a*, the application log, e.g. **112***a*, is in a format selected by the vendor for the logging purpose An application log **112** may contain application data in a proprietary data format, or may include or exclude certain types of log information, as designed by the application vendor Conventionally, no consistency or standardization or compatibility is expected or maintained between one application log, e g **112***a*, and another application log, e g **112***b*. Other software applications, including the context manager **100**, can thus not make use of application logs **112** unless specifically configured for particular expected formats and content

As more records are kept in electronic form and as the types of information retained in databases has proliferated, a concern has developed regarding the security and privacy of such information Privacy rights are an important factor in the design and operation of commercial, governmental, educational, financial and medical record keeping systems Legislation has been passed in some instances to protect consumer and patient records for example, and liability attaches to maintaining and using such data

The medical industry in particular views the safety and privacy of patient records as a public policy issue The Health Insurance Portability and Accountability Act of 1996 (hereinafter "the HIPAA") was passed by Congress to address such public policy issues, and lays out guidelines and requirements for institutions and entities in control of patient records and data

Presently, no satisfactory and efficient way is known to enable monitoring, auditing, enforcing or assessing compliance with local institutional policies or government regulations, especially across applications or platforms. Also lacking is any consistent approach to recording or controlling access to such sensitive data across applications executing on a data processing system. The absence of centralized logging and storage means useful to a broad spectrum of applications from a plurality of software application vendors is a continuing problem that binders or prevents streamlined data access management or auditing.

SUMMARY

Accordingly, some embodiments of the present invention are directed to a method for auditing data-access events occurring in a context management system, the method comprising: collecting context data from a plurality of applications that use the context management system; storing data corresponding to the collected context data on a centralized storage location; and extracting audit information by processing at least a subset of the data stored on the centralized storage location.

Other embodiments are directed to a method for storing context data, from a plurality of sources in a context management system, onto a centralized storage location, comprising: receiving context data from the plurality of sources; synchronizing the context data using a context manager; and storing the context data in the centralized storage location; wherein storing the context data is performed according to a synchronization scheme, that includes context data from at least two sources.

Another embodiment is directed to a method for controlling access to a stored data object, comprising: determining whether a data-access event is authorized under a predetermined rule, wherein a context manager is operable to allow or deny execution of said data-access event based on (i) context data, corresponding to the data-access event, and (ii) the predetermined rule.

Regarding the Health Insurance Portability and Accountability Act (HIPAA), some embodiments are directed to a method for assessing compliance with the HIPAA, in a context management system, the method comprising: collecting context data from a plurality of applications that use the context management system; storing data corresponding to the collected context data on a centralized storage location; and extracting audit information by processing at least a subset of the data stored on the centralized storage location, the audit information suitable for making an assessment of compliance with a provision of the HIPAA.

Additionally, some embodiments are directed to a method for auditing data access events in a data processing system, comprising: transferring context information from a first software application executing in the data processing system to a second software application executing in the data processing system; storing the context data in a centralized storage location; and extracting from the centralized storage location information indicative of data access events occurring in the data processing system.

Yet other embodiments are directed to a data processing system for auditing data access events in a context management framework, comprising: a plurality of software applications executing in the data processing system; a context manager coupled to the software applications that manages context data exchanges between the software applications; a centralized storage location, coupled to the context manager, that stores a central record of the context data exchanges; and an auditor, coupled to the centralized storage location, that retrieves information from the centralized storage location indicative of data access events occurring in the data processing system.

According to some embodiments, a machine-readable medium is provided, having thereon instructions, which when executed: collect context data from a plurality of applications that use a context management system; store data corresponding to the collected context data on a centralized storage location; and extract audit information by processing at least a subset of the data stored on the centralized storage location.

Yet other embodiments are directed to a method for identifying an application in a context management environment, wherein the application is coupled to a context manager, comprising: associating the application with an information tag when the application invokes a method that carries application-identifying information; augmenting a URL, passing between the context manager and the application, with the information tag, yielding a compound URL containing the URL and the information tag; parsing a communication from the application containing the compound URL to extract information corresponding to the information tag therefrom when the application invokes a method that does not carry application-identifying information; and looking up the identity of the application corresponding to the information tag.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a context management system according to the prior art;

FIG. **2** shows an exemplary data processing computer system and its primary components;

FIG. **3** shows an exemplary storage system which can be used with the computer system;

FIG. **4** shows an embodiment of a context management system according to the present invention;

FIG. **5** shows an embodiment of a context management system where data is formatted between two formats using a formatter;

FIG. **6** shows an embodiment of a context management system according to the present invention, including audit and archive capability;

FIG. **7** shows an embodiment of a context management system having some applications executing on a point-of-use machine and others executing on a remote server, with a network coupling various components of the system;

FIG. **8** shows an embodiment of a context management system which uses a rule set to control data-access events by a user, the figure also shows a monitor coupled to the system;

FIG. **9** shows an embodiment of a context management system having intermediate collection platforms or message queues;

FIG. **10** shows an embodiment of a synchronizer in a context management system which synchronizes context data for storage on a centralized storage location;

FIG. **11** shows an embodiment of a method for auditing and controlling data-access events.

FIG. **12** shows an embodiment of a context data processing and storage method.

FIG. **13** shows an embodiment of a context management system using a COM-to-Web proxy.

FIG. **14** shows a simplified embodiment of a method for communication and for identification of an application using a Web-proxy.

FIG. **15** shows an exemplary embodiment of a system using a Web-proxy to handle context management communications with a non-Web-based application.

FIG. **16** shows an exemplary embodiment of a system using a Web browser to handle context management communications with a Web-based application.

DETAILED DESCRIPTION

Various aspects of embodiments of the present invention address and remedy various shortcomings of presently-available systems either mentioned previously or as will become apparent to those skilled in the art upon review of this disclosure. Generally, control and auditing capabilities are provided for context management, and various other features and enhancements are also provided by the present context management architecture, to be described in more detail below. A non-exhaustive description of several aspects of embodiments of systems and methods follow, including a centralized storage architecture for context management, auditing of data from the centralized storage location, sometimes coupling the centralized storage location to the context manager over a network, synchronizing context data for delivery to and retrieval from the centralized storage location, collecting context data at intermediate collection platforms or message queues and buffers for use with the centralized storage architecture, and controlling access to data records and/or context data logged on the centralized storage location.

Many shortcomings of the prior art are remedied by use of a centralized storage location coupled to the context manager. While it is possible to still use the application-specific logs and application data records in their specialized or proprietary formats, the centralized storage coupled to the context manager enhances the functionality and usefulness of the context manager. In some embodiments, added capabilities are introduced as a result of having a consistent monolithic record of context events and data-access events in the centralized storage location. Examples of these added capabilities include multiple-application audit capability and access control.

The nature of the present invention will become apparent upon reading the description of the aspects of embodiments thereof, and especially when read in conjunction with the associated figures in which like elements are denoted by like reference numerals.

In some preferred embodiments, aspects of the present invention are carried out on a data processing system or on a computer system. A computer system **1300**, is shown in FIG. **2**. Various elements of the embodiments described herein, either individually or in combination, may be implemented on the computer system **1300**. Typically the computer system **1300** includes at least one main unit coupled, directly or indirectly, to one or more output devices **1301** which transmit information or display information to one or more users or machines. The computer system **1300** is also coupled, directly or indirectly, to one or more input devices **1302** which receive input from one or more users or machines. The main unit may include one or more processors **1303** coupled, directly or indirectly, to a memory system **1304** via one or more interconnection mechanisms **1305**, examples of which include a bus or a switch. The input devices **1302** and the output devices **1301** are also coupled to the processor **1303** and to the memory system **1304** via the interconnection mechanism **1305**. The computer system **1300** may further comprise a storage system **1306** in which information is held on or in a non-volatile medium. The medium may be fixed in the system or may be removable.

The computer system **1300** may be a general purpose computer system which is programmable using a computer programming language. Computer programming languages suitable for implementing such a system include procedural programming languages, object-oriented programming languages, macro languages, or combinations thereof. The computer system **1300** may also be specially-programmed, special-purpose hardware, or an application specific integrated circuit (ASIC).

In a general-purpose computer system, the processor **1303** is typically a commercially-available processor which executes a program called an operating system which controls the execution of other computer programs and provides scheduling, input/output and other device control, accounting, compilation, storage assignment, data management, memory management, communication and data flow control and other services. The processor and operating system define the computer platform for which application programs in other computer programming languages are written. The invention is not limited to any particular processor, operating system or programming language.

The storage system **1306**, shown in greater detail in FIG. **3**, typically includes a computer-readable and writeable nonvolatile recording medium **1401** in which signals are stored that define a program to be executed by the processor **1303** or information stored on or in the medium **1401** to be used by the program. The medium **1401** may, for example, be a disk or flash memory. Typically, in operation, the processor **1303** causes data to be read from the nonvolatile recording medium **1401** into another memory **1402** that allows for faster access to the information by the processor **1303** than does the medium **1401**. This memory **1402** is typically a volatile, random access memory (RAM), such as a dynamic random access memory (DRAM) or static random access memory (SRAM). It may be located in storage system **1306**, as shown in FIG. **3**, or in memory system **1304**, as shown in FIG. **2**. The processor **1303** generally manipulates the data within the integrated circuit memory **1304**, **1402** and then copies the data to the medium **1401** after processing is completed. A variety of mechanisms are known for managing data movement between the medium **1401** and the integrated circuit memory element **1304**, **1402**, and the invention is not limited thereto. The invention is also not limited to a particular memory system **1304** or storage system **1306**.

Aspects of embodiments of the invention may be implemented in software, hardware, firmware, or combinations thereof. The various elements of an embodiment, either individually or in combination, may be implemented as a computer program product including a computer-readable medium on which instructions are stored for access and execution by a processor. When executed by the computer, the instructions instruct the computer to perform the various steps of the process.

FIG. **4** shows an embodiment of a context management architecture which places the context manager **100** in between a plurality of context-enabled applications **110** and a centralized storage location **120**. This architecture allows for a streamlined uniform storage and access capability by the context management system. Note that applications **110** may retain and use their individual dedicated logs **112**, as described earlier with reference to FIG. **1**. In some embodiments, not all the data needed for some purpose will be store in the centralized storage location **120**, in which case the application logs **112** can be useful in providing functionality or data to augment information from the cen-

tralized storage location **120**. In order to achieve the architecture shown in FIG. **2**, some embodiments use a context management server (sometimes referred to as a "vault" or an "appliance") or other component of the context manager **100** to act as a collector for context data passing to and from various applications **110**. Once collected, context data may be sent through message queues and/or synchronizers to the centralized storage location **120**. Reference is made to U.S. patent application Ser. Nos. 60/136,670, 60/139,235, 60/254,753, 09/545,396 and 09/583,301, which provide disclosure of subject matter related to context management systems, and all of which are hereby incorporated by reference.

The centralized storage location **120** may be structured, and organized according to any of numerous ways known to those skilled in the art of data storage. Examples of the centralized storage location **120** include file systems and databases. Databases suitable for use with the present invention include, but are not limited to, relational databases, hierarchical databases, networks and directory systems. The information kept on the centralized storage location **120** may be formatted or modified for example by compression to improve economy or using another data processing technique to improve efficiency or performance of the storage system.

It should be noted that the data stored on the centralized storage location **120** is not constrained to explicit storage of context data per se. The data stored on the centralized storage location **120** may be data corresponding to the context data or parts thereof. That is, a formatter or data translator may be employed in the context manager **100** and/or in the centralized storage location **120** which is adapted to convert data from one data format to another. For example, in a system supporting the CCOW standard set and data compatible therewith, a formatter **230** may be employed to convert data between a first data format and a second format compatible with the CCOW standard set.

FIG. **5** shows a formatter **230** disposed between the context manager **100** and the centralized storage location **120**. CCOW-compliant data **310** is used in the context management system by the context manager **100**, but the centralized storage location **120** only sends and receives data **320** formatted in a database-specific data format. The formatter **230** may be implemented in the context manager **100** or in another component suitable for carrying out the formatting operations.

It should also be understood that some communication events and data transfer events carried out according to some aspects of embodiments of the present invention may be done securely. Secure communication between any of the components, applications, or storage devices may be optionally implemented as a mode of operation, thus allowing non-secure and secure context management operations.

Further, the applications **110** may still remain coupled to their respective individual vendor-specific logs **112** as described earlier.

FIG. **6** shows an embodiment of a context management system as described above, but further having an archive storage location **122** coupled to the centralized storage location **120**. While configurable in many ways, an archive can serve to relieve the primary centralized storage location **120** of old data, or data not in active use, allowing the centralized storage location **120** to delete or overwrite old or unused data. Since context management systems can be expected to accumulate a large amount of stored information over time, archival capability may become necessary if the centralized storage location **120** nears or reaches its capacity. The archive storage location **122** can then in turn be coupled to other backup or auxiliary archive devices, such as tapes, digital storage media, or other printed or electronic forms of record keeping. The archive storage location **122** does not necessarily reside in any predetermined location or arrangement relative to the centralized storage location **120**. In fact, the archive storage location **122** may be implemented as a plurality of storage locations which may be distributed or only temporarily coupled to the overall system for transfer of data from the centralized storage location **120** back and forth to the archive storage location **122**.

It is often, but not always, necessary to have the system be able to transfer data both to and from the archive storage location **122** when necessary. Thus it is useful in some cases to incorporate retrieval capability to retrieve archived data from the archive storage location **122** back into the centralized storage location **120** for use by the context manager **100** or other elements coupled thereto.

The embodiment of FIG. **6** also shows an auditor **130** coupled to the centralized storage location **120**. The auditor is capable of accessing and processing data from the centralized storage location **120**. As an example of the many possible uses for the auditor **130**, periodic audits by the auditor **130** can be conducted to assess an organization's compliance with local organization policies or its adherence to statutory requirements. As a specific example, a hospital using a context management system and having a centralized storage location **120** may conduct periodic audits using the auditor **130** to parse through context data or other data stored on the centralized storage location **120**. Such audits may be conducted by the auditor **130** or another auxiliary module coupled thereto, and send summary reports or other conclusory information to an output device or to another machine or to another destination that can make use of and interpret such information.

The auditor **130** may be equipped with software to generate automatic reporting sheets, signals, tables, or data objects indicative of the organization's compliance with its own policies or with applicable laws. Additionally, detailed reports on the usage of a hospital's patient medical records or accounting records by particular users may be generated. If a particular hospital employee comes under suspicion for acting in a way that is in violation of the policies or laws mentioned above, an audit can be performed, including an audit report, containing information showing which context data was associated with that employee. This information may then reveal whether or not the employee improperly accessed certain information or used certain applications in violation of applicable policies and rules as described above.

Similarly, an audit may be performed and an audit report generated to indicate what context-related activity has taken place on the system relevant to a particular patient's records. According to one aspect of this embodiment, the centralized storage location **120** stores such information in a way which is searchable and cross-referenced. Therefore the auditor **130** can generate a variety of customized audits depending on the need.

It is important to mention that the process of collecting, storing, or subsequently auditing information is not limited to collecting, storing and auditing context data. Data-access events generally are so recordable and auditable. These data-access events can comprise any of at least: context data, certain types or subsets of context data (i.e. not all available or collected context data), context data items (e.g., user, patient), context gestures, application data access, and

attempted data-access events (insofar as they are identifiable and translate into meaningful signals). Thus a "data-access event" is almost any event corresponding to an action by a user or a machine which causes data (including context and application data) to be moved from one location to another or to be retrieved from memory.

In addition, not all of the collected context data needs to be stored into the centralized storage location **120**. In some instances only a subset of the context data is stored. Considerations of computational resources, execution speed, efficiency and privacy may influence the decision on what context data to collect or store.

FIG **7** shows an embodiment of a context management system having an architecture using a network **150** adapted for carrying communication signals, data, and other information from one location to another. While still employing the context manager **100** to conduct context transactions between a plurality of applications **110**, the applications **110** may not all be executing on the same machine on which the context manager **100** runs. Thus, if the context manager **100** is executing on a point-of-use machine **140**, and applications **110***a* and **110***b* are also executing on the point-of-use machine **140**, a third application **110***c* may execute on a remote server **160**, coupled to the point-of-use machine **140** and the context manager **100**, by a network **150**. The context manager **100** may also use the network **150**, or another network coupled thereto, to reach the centralized storage location **120**.

Secondary or auxiliary networks and other machines may be connected in a complex architecture as is known to those skilled in the art of networking. In fact, an entire enterprise (e.g., a hospital) may be coupled to a few or even a single context manager **100**. The entire enterprise may then use the services of the centralized storage location **120**. Various considerations, including reliability and security, may dictate using a number of storage locations, which when taken together form the centralized storage location **120**. It is not necessary to have a single disk drive or tape device or other storage device acting as the centralized storage location **120**. Instead, it is possible to employ subsystems, which need not be of the same type, to serve as the centralized storage location **120**.

The context manager **100** itself may run as a software application executing on a local point-of-use machine **140**, or may be executed as an applet in a frame on the desktop of the point-of-use machine **140**. The context manager **100** may itself be executing on a remote web server such as the remote server **160**.

The ability to access and audit the contents of the centralized storage location **120** opens up new possibilities for enhancing the functionality of context management systems. Since the data stored on the centralized storage location **120** is uniformly-accessible to the auditor **130**, the auditor **130** may trigger, based on some criterion, a particular subsequent decisional act. For example, a decision can be made automatically or by a "monitor," which can be a human or a machine, that acts or is informed upon execution or attempted execution of a certain context gesture. As an example, a member of a hospital's accounting department may not have authorization to access patient medical records. A determination of such access may be made by comparing an attribute of the user who is logged into the system with a list of attributes of those forbidden to access patient medical records. A code or other identifying feature, such as user name or employee ID number, can be compared with an index of hospital employees who are allowed to access patient medical records. Even more specifically, it may be decided by local policy that only physicians treating particular patients may have access to those particular patients' medical records. Analogously, a physician handling one aspect of a patient's healthcare, e.g., respiratory conditions, may be barred from modifying or accessing patient medical records having to do with the patient's other medical conditions, e.g., mental health.

It is possible, based on output from the auditor **130**, to then trigger a message to the user informing the user of a particular condition. For example, an alert may be presented to a caregiver if a certain patient has a medical condition warranting special care in certain circumstances. As a specific example, a pharmacy employee at the hospital who conducts a context gesture to fill a prescription for a certain patient may be presented with a message reciting known allergies for that particular patient. The warning message or alarm may be triggered by the pharmacy employee performing a context gesture that involved the particular patient with the allergies. That is to say that the present invention provides, in some embodiments facilitating audit and/or context-driven controls, for decisional and other actions to be undertaken or initiated based on context data.

Output from the auditor **130** may be sent to a machine or human monitor, who will take some action in the event that a certain unauthorized data access event has taken place or an attempt to perform such an unauthorized act has taken place. A more complete description of embodiments using a monitor will be given below.

Authorization and access control may be conducted with or without an auditor **130**. FIG **8** shows an embodiment of a context management system having authorization and access control capability. In this example, a plurality of applications **110** exchange context data through a context manger **100** as before. The context manager **100** may be coupled to a centralized storage location **120** as described earlier, and other features of that architecture as described above are possible. However, in this embodiment, an authorizer **160** receives context data or data corresponding to context gestures and performs a determination of whether the context gestures are authorized. The authorizer **160** has access to look-up tables or rule sets **200** to make the decision whether a context gesture is authorized or not. The rule set or look-up tables **200** may be coupled to or incorporate enterprise-wide local policy rules or tables **210** and legislative provisions or statutes or other rule-based criterion **220**.

The concept given above may be generalized so that rule-based decisions include all means for arriving at a decision. A "rule" can hence be considered for our purposes to encompass at least: an algorithmic or logical operation, a table whose contents form a rule, etc. A look-up table (LUT) is an example of such a rule, usually stored in memory. An algorithm for making a decision on the basis of a mathematical calculation is another rule accessible to a context management system.

The authorizer **160** provides an output to an access controller **170** which is adapted for controlling permission to perform a context gesture or other act. If authorization is declined by the authorizer **160** for a particular context gesture, the access controller **170** may send or decline to send a signal to the context manager **100**, implementing the access control decision. Alternately, a signal containing the results of an authorization check can be sent to the context manager **100**, which will then implement the access control. The context manager **100** may accomplish this by incorporating sub-modules which implement the functions of the

authorizer **160** and/or the access controller **170** as described above. However, this functionality may also be built into other modules which may execute on any of the machines in the context management system.

Once a decision is made on whether to allow a particular context gesture, this often implies a determination of whether the associated data record access is authorized and can be carried out In our previous example, an accountant who is attempting to access a patient's mental health records may be barred from viewing the medical record as a consequence of being barred from executing the corresponding context gesture

In addition to merely denying or allowing the execution of a context gesture or a data record access event, the access controller **170** and/or authorizer **160** may provide a signal to a monitor **180**. The monitor **180** may itself cause or send signals, such as alarm signals or signals that shut down a system or activate another system. The monitor **180** may be implemented in numerous ways These include implementation as an electronic mail server adapted to sending an electronic mail message to an administrator, alerting the administrator of a breech The monitor **180** may similarly be a telephony or paging server, adapted for delivering a telephone or pager message to an administrator or other security personnel. The monitor **180** may in addition be an alarm device, such as an audible or a visual alarm. The monitor **180** can also be a human operator who can make decisions based on an alarm signal or other message from the monitor **180**.

In some embodiments, the authorizer **160** may be coupled to the centralized storage location **120**, and receive its input from the centralized storage location **120** rather than from the context manager **100**

FIG. **9** shows an embodiment of a context management system employing intermediate collection platforms **400** and/or message queues The context-enabled applications **110** exchange context data through the context manager **100** The intermediate collection platforms may be storage locations or buffers, implemented in hardware and/or in software, optionally as part of the context manager **100** The intermediate collection platforms may comprise message queues. The message queues are in turn coupled to the centralized storage location **120**.

Many other architectures, including distributed architectures at the local and global level, may add functionality to the system and methods described by the present invention

FIG. **10** shows a synchronizer **420**, which may be implemented separately or as part of a context manager **100**, for use in a context management system A plurality of applications **110** receive and send context data to the synchronizer **420**. In order to effect a smooth and organized storage onto and retrieval from the centralized storage location **120**, the synchronizer **420** uses a synchronization scheme adapted for organizing the incoming context data into a single stream of data for storage onto the centralized storage location **120**. The synchronization scheme may comprise a chronological scheme, wherein messages and data arriving at the synchronizer **420** are placed in the proper order for storage on to the centralized storage location **120** Tags appended to, or other criterion can be used as synchronizing schemes

One aspect of this exemplary embodiment of the present invention is that it allows for a scaleable architecture It can be especially advantageous in enterprise-wide systems to have context management with a centralized storage location **120** as described above. However, if the number of machines, including servers and point-of-use machines proliferates, it may be efficient to carry out the clustering described herein so that the overall architecture remains compatible with the concept of centralized storage As described previously, the centralized storage location **120** itself may be clustered or formed of smaller sub-systems that are then organized logically using a single index

FIG. **11** shows an exemplary method carried out according to some embodiments of the present invention In act **1000**, context data is collected from a plurality of applications. In act **1005**, data corresponding to the collected context data, which may include data identical to the collected context data, is stored on a centralized storage location Optionally, collecting the context data as in act **1000** may comprise appending and/or exchanging a compound URL with one or more applications, as shown in act **1015**. Also, data may be converted between two different data formats, as shown in act **1020**.

Once collected data is stored on the centralized storage location, at least a subset of the stored data is extracted and/or processed to obtain audit information according to act **1010**.

The extracted data from act **1010** may be used for comparison against a rule available to the context management system, such as a lookup table or an algorithm, in act **1035** The extracted data may also be evaluated for assessing compliance with a policy or regulation, such as the HIPAA, as shown in act **1040**.

The exemplary embodiment also shows in act **1030** a determination of whether a particular data-access event is authorized. This is possibly done using an authorizer as part of or in conjunction with the context manager, and may base the determination on a comparison of some data from the context data and the set of rules accessible to the authorizer.

The method also shows, in act **1045**, an access control step which can allow or deny execution of an access-control event or act by a user as described earlier. An access controller may be used to enforce the access control and a monitor may be informed or activated responsive to the authorization and access control status

FIG. **12** shows an exemplary embodiment of a method for processing context data in a context management system such as those given in the previous discussion. The method comprises receiving context data from a plurality of sources in act **2000**. The context data are synchronized according to a synchronization scheme, possibly using a synchronizer, in act **2005**. The data having been synchronized is stored in a centralized storage location in act **2010**

Optionally, the data may be stored on intermediate storage locations, which may be clustered storage devices sharing a single directory, as shown in act **2015**. Also, the data may be converted between one data format and another as in act **2020** prior to storing onto the centralized storage location.

The CCOW standard supports collections of methods known as interfaces, which include secure and non-secure interfaces. Various methods are carried out by context-enabled applications within the framework of the interfaces The applications exchange parameters and data with the context manager when using the context management system. The exchanged parameters and data can include application identification (ID) information, Uniform Resource Locators (URLs) and other information According to the CCOW standard, not all methods are required to provide the identity of the application to the context manager This can compromise the auditing ability of an auditor by failing to provide all (e g , application-identifying) data for the activity record or log used by the auditor. A solution to this

problem is presented below and briefly explained using exemplary embodiments that are intended to clarify the solution but are not intended to be limiting.

Context-enabled applications almost always invoke a "Join" method, or another identifying method, that includes application-identifying information, prior to beginning context transactions with the context manager. In some embodiments, applications use a Web-based interface to exchange URL data with the context manager in the course of conducting context-related transactions. These applications invoke a method, such as the "Locate" method, which provides them with the location of the context manager or its URL. Other applications, e g , COM-based applications and non-Web-based applications, do not exchange URL data with the context manager. Even some Web-based applications carry out methods that do not include application-identifying information in their communications.

Accordingly, some embodiments of the present invention are directed to a Web-proxy, e g., a COM-to-Web proxy, which provides HTTP calls and URLs for identifying those applications which do not normally identify themselves in their communication with the context manager or which are carrying out methods that do not include application-identifying information. The context manager's URL may be augmented or decorated with extra appended information including application-identification "tags." This appended ID tag information may be suitable for identifying the applications where the applications would otherwise be unidentified to the context manager.

One implementation of the above concept involves having the context manager append an ID tag to its URL, thus forming a compound URL. The context manager then passes the compound URL, having the ID tag appended thereto, to the application requesting the context manager's services. The application will then include the compound URL in the communications and request messages and responses it exchanges with the context manager. Since the compound URL includes the ID tag information, the context manager will be able to associate, e g , using a lookup table, which application is conducting a given context transaction or method, even if the method does not explicitly require the use of application-identifying information.

It should be understood that this concept is not limited to CCOW COM-based applications, but can be extended to other Web-based and non-Web-based applications as well. In addition, it should be understood that a compound URL can be formed by including or appending URL data that not only signifies application-identifying information, but also can carry out an unlimited number of other useful auxiliary functions that require passing data between an application invoking a method and the context manager. This means that applications are not limited to exchanging the information defined by the method, but rather, by using the proxy, the applications can exchange a broad spectrum of information with the context manager. Some of this augmenting information carried in the compound URL may then be used for audits or other functions, or may be passed on to other applications.

FIG. **13** shows an embodiment of a context management system using a COM-to-Web proxy **500** for allowing the context manager to identify communications from a non-Web-based application **111** that does not provide its identity to the context manager **100**. The context manager **100** exchanges information, including URL information **510** and URL-augmenting information **520** through a Web interface **540** with context-enabled applications **111**, **113**. A first application is a Web-based application **113** and exchanges URL information **510** with the context manager as usual. Other information customary to the various method operations is not shown in the figure.

A second application is a non-Web-based application **111**. This application exchanges information, including a compound URL **525**, consisting of URL information **510** and URL-augmenting information **520**, with the COM-to-Web proxy **500**. The COM-to-Web proxy **500** handles the communication with the Web interface **540**. The system thus even supports applications that would normally not identify themselves, and the context manager according to this embodiment can determine the identity of any such applications, even if they are using methods which normally would not include application-identifying information.

FIG. **14** shows a method carried out in a multi-layer context management environment. Here a Web-proxy is used to convert communications from a first non-Web-based layer, using a non-HTTP protocol, to and from a second, Web-based, layer using the HTTP protocol. In act **3000**, a non-Web-based application uses a "Join" method that includes application-identifying information. The context manager appends an ID tag in act **3005** to the context manager's URL to yield a compound URL, which will identify the application in future transactions with the context manager. The application uses the compound URL for subsequent communications through the Web-proxy to the context manager in act **3010**. These communications now having the ID tag appended thereto in a way that allows the context manager to identify the application, possibly using a lookup table, as in act **3015**.

FIG. **15** shows a context management system and sequence of acts and/or communications according to one embodiment of the present invention. A point-of-use device **140** has a non-Web-based application **111** and a Web-proxy **500** and a CCOW context registry **114** executing thereon. Communications are carried out with a context manager **100** coupled to a centralized storage location **120** such as a database.

A "Join" method is invoked and an application-identifying signal **3100** is sent from the non-Web-based application **111** to the Web-proxy **500**. The Web-proxy **500** sends a "Locate" signal or method communication **3102** to the CCOW context registry **114**. Next, the CCOW context registry **114** obtains the context manager's URL by sending a signal **3104** and receiving a signal **3106** comprising the compound URL with an application ID tag. Resources are also allocated for the application **111** by the context manager **100**.

The Web-proxy **500** sends a "Join" signal **3110** to the context manager **100**, which associates the application **111** identity with the ID tag and returns a coupon to the Web-proxy **500** in signal **3112**. The coupon is given to the application **111** by the Web-proxy **500** in signal **3114**.

Subsequently, the application **111** may invoke non-identifying methods with signal **3116**. The information therein is sent to the context manager **100** in signal **3118**. A return from the context manager **100** is provided to the application **111** via the Web-proxy **500** in signals **3122** and **3124**, respectively.

Note that the context manager **100** records the application **111** requests and other information onto the centralized storage location **120** as described in previous embodiments.

FIG. **16** shows an exemplary diagram with elements and signals for carrying out a method according to the present invention used by Web-based applications using non-identifying methods.

A Web-server **145** executing a Web-based application **113** is linked with a context manager **100** and a point-of-use device **140** executing a Web browser **501** and a CCOW context registry **114**

On initiating activity, such as by using a "Start Page" event **4100**, the Web browser **501** uses a "Locate" method via the CCOW context registry **114** to obtain the context manager's URL and an application ID tag in a compound URL in signals **4102**, **4104** and **4106** The compound (or decorated) URL is returned to the Web browser **501** in signal **4108**, which is in turn returned to the application **113** in signal **4110** The application **113** can use a "Join" method in **4112** to get a coupon from the context manager **100** in signal **4114** Once it receives the coupon, the application **113** is free to carry out non-identifying methods in communications carrying the compound URL and the ID tag information in signals **4116** and **4120**

As before, the context manager **100** records the application **113** requests and other information onto the centralized storage location **120**

Therefore, and in view of the above description and accompanying drawings, a context management framework is given that provides in various embodiments, numerous advantages over previously-existing systems In some instances, an architecture having a centralized storage location coupled to a context manager is provided for servicing and logging context events from a plurality of sources This type of system uses a synchronization scheme to perform orderly storage and retrieval of data to and from the centralized storage location In other instances, information stored in the centralized storage location or signals from the context manager are used to achieve an auditing capability for reviewing and acting on context data events and gestures Selective blocking or allowance of impending context gestures is accomplished based on a rule set or lookup table containing rules or other data to make such access control decisions Access to sensitive data and other security measures may thus be implemented using the teachings presented herein

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications, and improvements will readily occur to those skilled in the art Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and scope of the invention Accordingly, the foregoing description is by way of example only and is limited only as defined in the following claims and the equivalents thereto

What is claimed is:

1 In a system comprising at least two software applications, a context manager which facilitates a sharing of a context among the at least two software applications in accordance with the Clinical Context Object Workgroup (CCOW) standard, a centralized database accessible to the context manager, and an auditor which provides an interface to enable the extraction of information from the centralized database relating to attempts to access patient data by the at least two software applications, a method comprising acts of:

(A) storing, in the centralized database, information relating to attempts to access patient data by the at least two software applications; and

(B) extracting, by the auditor, at least some of the information stored in the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA)

2 The method of claim **1**, wherein the act (B) comprises extracting information relating to at least one attempt to access patient data that is unauthorized via at least one rule

3 The method of claim **2**, wherein the at least one rule is specified by the at least one provision of HIPAA

4 The method of claim **2**, wherein when the extracted information indicates that at least one unauthorized attempt was made to access patient data, the method further comprises an act of:

(C) creating a report comprising an alert indicating that the unauthorized attempt was made to access patient data

5 The method of claim **1**, wherein the patient data includes data relating to at least a first patient, and the information extracted from the centralized database in the act (B) comprises information relating to attempts to access the data relating to the first patient.

6 The method of claim **1**, wherein the act (A) comprises an act of storing information, relating to attempts to access patient data, that is provided by the at least two software applications

7 A system for auditing attempts to access patient data in a computer system comprising at least two software applications operable to access patient data and a context manager which facilitates a sharing of a context among the at least two software applications in accordance with the Clinical Context Object Workgroup (CCOW) standard, the system comprising:

a centralized database that stores information relating to attempts to access patient data by the at least two software applications; and

an auditor that provides an interface to enable an extraction of at least some of the information from the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA).

8 The system of claim **7**, further comprising a report facility that creates at least one report, based upon the extracted information, which presents information relating to attempts to access patient data by the at least two software applications

9 The system of claim **8**, wherein the system further comprises an alert facility which sends an alert to a user when it is determined that an attempt unauthorized by at least one HIPAA provision was made to access patient data

10 The system of claim **8**, wherein the patient data includes data relating to a first patient, and the at least one report includes information extracted from the centralized database on attempts to access the data relating to the first patient.

11 The system of claim **7**, wherein the auditor interface further enables the extraction of at least some of the information from the centralized database relating to attempts to access patient data that are unauthorized by the at least one HIPAA provision

12 The system of claim **7**, wherein the information relating to attempts to access patient data is provided by the at least two software applications to the centralized database

13 At least one computer readable medium encoded with instructions for execution in a computer system comprising at least two software applications, a context manager which

facilitates a sharing of a context among the at least two software applications in accordance with the Clinical Context Object Workgroup (CCOW) standard, a centralized database accessible to the context manager, and an auditor which provides an interface to enable the extraction of information from the centralized database relating to attempts to access patient data by the at least two software applications, the instructions, when executed on the computer system, perform a method comprising acts of:

(A) storing, in the centralized database, information relating to attempts to access patient data by the at least two software applications; and

(B) extracting, by the auditor, at least some of the information stored in the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA).

14. The at least one computer readable medium of claim **13**, wherein the act (B) comprises extracting information relating to at least one attempt to access patient data that is unauthorized via at least one rule.

15. The at least one computer readable medium of claim **14**, wherein the at least one rule is specified by the at least one provision of HIPAA.

16. The at least one computer readable medium of claim **14**, wherein when the extracted information indicates that at least one unauthorized attempt was made to access patient data, the method further comprises an act of:

(C) creating a report comprising an alert indicating that the unauthorized attempt was made to access patient data.

17. The at least one computer readable medium of claim **13**, wherein the patient data includes data relating to at least a first patient, and the information extracted from the centralized database in the act (B) comprises information relating to attempts to access the data relating to the first patient.

18. The at least one computer readable medium of claim **13**, wherein the act (A) comprises an act of storing information, relating to attempts to access patient data, that is provided by the at least two software applications.

19. The at least one computer readable medium of claim **13**, wherein the centralized database provides a single interface to the auditor to enable the extracted data to be extracted via the single interface.

20. In a system comprising at least two software applications capable of accessing patient data, a centralized database, and an auditor that is coupled to the centralized database, a method comprising acts of:

(A) storing, in the centralized database, information relating to attempts to access patient data by the at least two software applications; and

(B) extracting, by the auditor, at least some of the information stored in the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA).

21. The method of claim **20**, wherein the act (B) comprises extracting information relating to at least one attempt to access patient data that is unauthorized via at least one rule.

22. The method of claim **21**, wherein the at least one rule is specified by the at least one provision of HIPAA.

23. The method of claim **21**, wherein when the extracted information indicates that at least one unauthorized attempt was made to access patient data, the method further comprises an act of:

(C) creating a report comprising an alert indicating that the unauthorized attempt was made to access patient data.

24. The method of claim **20**, wherein the patient data includes data relating to at least a first patient, and the information extracted from the centralized database in the act (B) comprises information relating to attempts to access the data relating to the first patient.

25. The method of claim **20**, wherein the act (A) comprises an act of storing information, relating to attempts to access patient data, that is provided by the at least two software applications.

26. A system for auditing attempts to access patient data in a computer system comprising at least two software applications operable to access patient data, the system comprising:

a centralized database that stores information relating to attempts to access patient data by the at least two software applications; and

an auditor that provides an interface to enable an extraction of at least some of the information from the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA).

27. The system of claim **26**, further comprising a report facility that creates at least one report, based upon the extracted information, which presents information relating to attempts to access patient data by the at least two software applications.

28. The system of claim **27**, wherein the system further comprises an alert facility which sends an alert to a user when it is determined that an attempt unauthorized by at least one HIPAA provision was made to access patient data.

29. The system of claim **27**, wherein the system further comprises a graphical user interface (GUI), and wherein the report is presented to a user via the GUI.

30. The system of claim **27**, wherein the patient data includes data relating to a first patient, and the at least one report includes information extracted from the centralized database on attempts to access the data relating to the first patient.

31. The system of claim **26**, wherein the auditor interface further enables the extraction of at least some of the information from the centralized database relating to attempts to access patient data that are unauthorized by the at least one HIPAA provision.

32. The system of claim **26**, wherein the information relating to attempts to access patient data is provided by the at least two software applications to the centralized database.

33. At least one computer readable medium encoded with instructions for execution in a computer system comprising at least two software applications capable of accessing patient data, a centralized database, and an auditor that is coupled to the centralized database, the instructions, when executed on the computer system, perform a method comprising acts of:

(A) storing, in the centralized database, information relating to attempts to access patient data by the at least two software applications; and

(B) extracting, by the auditor, at least some of the information stored in the centralized database relating to attempts to access patient data by the at least two software applications, the at least some of the information being suitable for making an assessment as to compliance with at least one provision of the Health Insurance Portability and Accountability Act (HIPPA).

34. The at least one computer readable medium of claim 33, wherein the act (B) comprises extracting information relating to at least one attempt to access patient data that is unauthorized via at least one rule.

35. The at least one computer readable medium of claim 34, wherein the at least one rule is specified by the at least one provision of HIPAA.

36. The at least one computer readable medium of claim 34, wherein when the extracted information indicates that at least one unauthorized attempt was made to access patient data, the method further comprises an act of:

(C) creating a report comprising an alert indicating that the unauthorized attempt was made to access patient data.

37. The at least one computer readable medium of claim 33, wherein the patient data includes data relating to at least a first patient, and the information extracted from the centralized database in the act (B) comprises information relating to attempts to access the data relating to the first patient.

38. The at least one computer readable medium of claim 33, wherein the act (A) comprises an act of storing information, relating to attempts to access patient data, that is provided by the at least two software applications.

39. The at least one computer readable medium of claim 33, wherein the centralized database provides a single interface to the auditor to enable the extracted data to be extracted via the single interface.

* * * * *

EXHIBIT 2

US006993556B1

(12) **United States Patent**
Seliger et al.

(10) **Patent No.: US 6,993,556 B1**
(45) **Date of Patent: Jan. 31, 2006**

(54) **CONTEXT ADMINISTRATOR**

(75) Inventors: **Robert Seliger**, Winchester, MA (US); **Elaine Seliger**, Winchester, MA (US); **David Fusari**, Groton, MA (US)

(73) Assignee: **Sentillion, Inc.**, Andover, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U S C. 154(b) by 0 days

(21) Appl No : **09/545,396**

(22) Filed: **Apr. 7, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/128,145, filed on Apr 7, 1999, provisional application No. 60/135,907, filed on May 25, 1999, provisional application No. 60/136,670, filed on May 28, 1999, provisional application No. 60/139,235, filed on Jun. 14, 1999, provisional application No. 60/139,145, filed on Jun. 14, 1999, provisional application No. 60/146,722, filed on Aug. 2, 1999, provisional application No. 60/145,681, filed on Jul. 26, 1999.

(51) **Int. Cl.**
G06F 15/16 (2006 01)

(52) **U.S. Cl.** **709/203**; 709/217; 709/219; 718/107; 718/108; 705/3; 705/4

(58) **Field of Classification Search** 709/202–203, 709/217, 219, 229; 718/107–108; 705/2, 705/3–4

See application file for complete search history.

(56) **References Cited**

U S. PATENT DOCUMENTS

5,491,817	A *	2/1996	Gopal et al	707/200
5,805,786	A	9/1998	Badovinatz et al	395/182.02
6,064,973	A *	5/2000	Smith et al	705/7
6,119,145	A *	9/2000	Ikeda et al	709/203
6,134,594	A *	10/2000	Helland et al	709/229
6,205,476	B1 *	3/2001	Hayes, Jr	709/220
6,237,092	B1 *	5/2001	Hayes, Jr	713/100
6,260,021	B1 *	7/2001	Wong et al	705/2
6,377,994	B1 *	4/2002	Ault et al	709/229
6,401,138	B1 *	6/2002	Judge et al	719/328
6,510,466	B1 *	1/2003	Cox et al	709/229

FOREIGN PATENT DOCUMENTS

EP 0 803 808 A 10/1997

OTHER PUBLICATIONS

Context Management ("CCOW") Specification Subject Data Definitions, Version CM-1 1, Nov. 6, 1999, pps. 1-28.
Context Management ("CCOW") Specification User Interface: Microsoft Windows, Version CM-1.1, Nov. 6, 1999, pps. 1-18.
Context Management CCOW Specification Component Technology Mapping: Active X, Version CM-1 1, Nov. 6, 1999, pps. 1-48.
Context Management (CCOW) Specification Technology- and Subject -Independent Component, Architecture Version CM-1 1, Nov. 6, 1999, pps. 1-228.
David Adams, "Solstice- Access System Administration Tools With a Graphical User Interface", XP002154495, (1995)

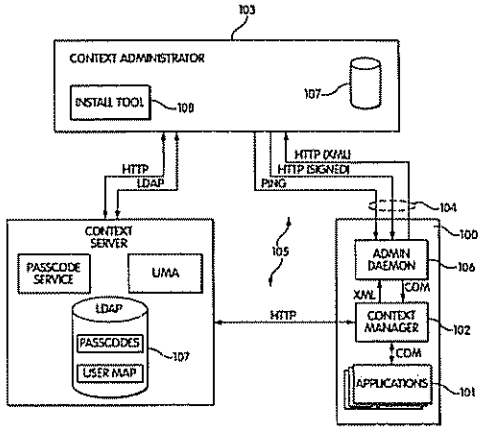
(Continued)

Primary Examiner—Ario Etienne
Assistant Examiner—LaShonda Jacobs
(74) *Attorney, Agent, or Firm*—Wolf, Greenfield & Sacks, P.C.

(57) **ABSTRACT**

A context management and administration system includes a context manager, which manages the context of plural applications programs, and an administration suite, which oversees and manages the manager. Context administration can include setting up and maintaining subject data definitions, intervening in context manager operations, providing security functions to protect sensitive context information against tampering by unauthorized users, etc.

32 Claims, 1 Drawing Sheet



OTHER PUBLICATIONS

David Adams, "Lpstat-Print Information about the Status of the Print Service", XP002154496 (1995).
David Adams, "Cancel-Cancel Print Request", XP002154497 (1995)
David Adams, "Lpshut-Stop the LP Print Service", XP002154498 (1995)
David Adams, "Ifconfig-Configure Network Interface Parameters", XP002154499 (1995)
Grubb et al , "Single Sign-On and the System Administrator", XP002154500 (1998)
David Adams, "Intro, Intro-Introduction to Maintenance Commands and Application Programs", XP002154501 (1995)
Clinical Context Working Group: "The Clinical Context Object Workgroup: Its Standard and Methods", XP002154044, (1998).

* cited by examiner

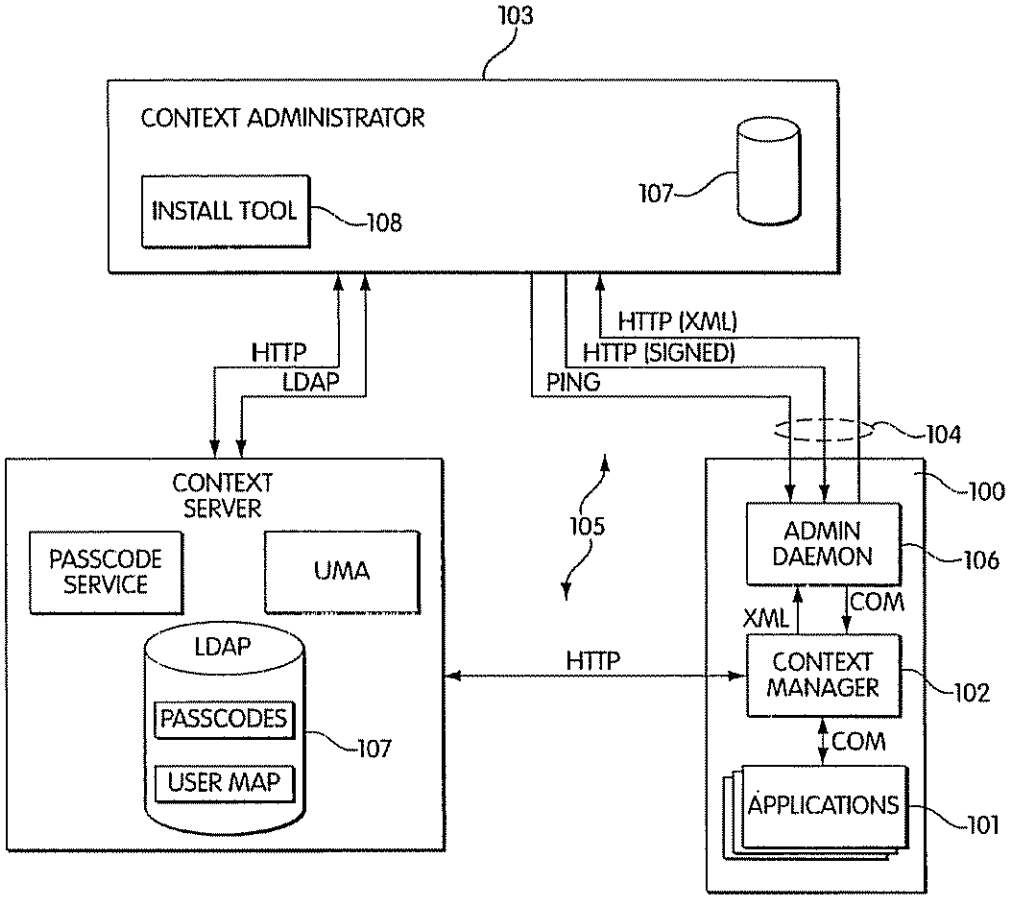

103
CONTEXT ADMINISTRATOR
INSTALL TOOL
108
107
HTTP
LDAP
HTTP (XML)
HTTP (SIGNED)
PING
104
CONTEXT SERVER
PASSCODE SERVICE
UMA
LDAP
PASSCODES
USER MAP
107
105
100
ADMIN DAEMON
106
XML
COM
HTTP
CONTEXT MANAGER
102
COM
APPLICATIONS
101

Fig. 1

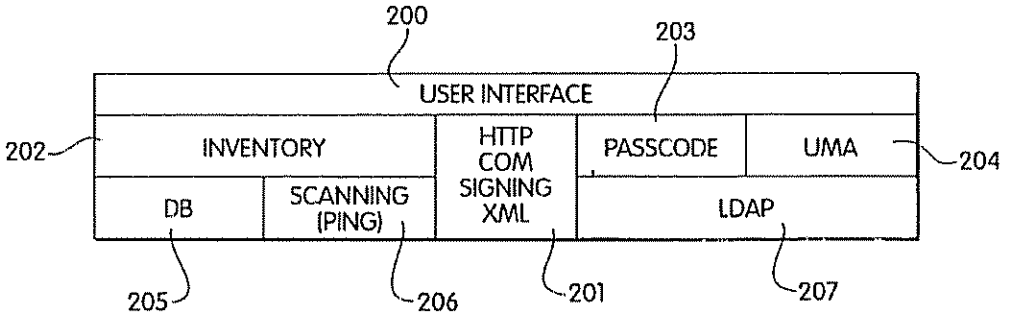

200
203
USER INTERFACE
202
INVENTORY
HTTP
COM
SIGNING
XML
PASSCODE
UMA
204
DB
SCANNING (PING)
LDAP
205
206
201
207

Fig. 2

CONTEXT ADMINISTRATOR

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims domestic priority under 35 U.S.C. § 119(e) to provisional U.S. patent application Ser. No. 60/128,145 filed Apr. 7, 1999, Ser. No. 60/135,907 filed May 25, 1999, Ser. No. 60/136,670 filed May 28, 1999, Ser. No. 60/139,235 filed Jun. 14, 1999, Ser. No. 60/139,145 filed Jun. 14, 1999, Ser. No. 60/146,722 filed Aug. 2, 1999, and Ser. No. 60/145,681 filed Jul. 26, 1999, all now abandoned, and incorporated herein in their entirety by reference.

FIELD OF THE INVENTION

The present invention relates to tools for managing and administering the management of context in software applications.

BACKGROUND OF THE INVENTION

There are many businesses or fields of endeavor, which rely on the use of plural desktop computer applications. One such field is the modern practice of medicine. In such a setting, users quite often find themselves entering and reentering similar information over and over. For example, a single user may have to repeat login information in plural applications, followed by the same or similar client information. Such information, that defines the environment in which each application operates is known as context. That is, context is a collection of data items and corresponding values, wherein the items represent information required in common between plural applications in an industry or business setting. For example, in health care, a patient identifier (patient ID) is an item which is part of the context in which plural clinical applications may participate, or share.

In the modern practice of medicine, a physician or other professional or staff member may need to store, retrieve, analyze, etc. various types of patient data. The patient data to be processed may be clinical; e.g. x-ray images or blood work results, or may be financial, e.g. insurance cover and billing history. Thus, clinical applications, such as those to store, retrieve and display x-ray images and those to store, retrieve and display blood work results have inputs and outputs which fall into two broad classes: highly specialized, work product specific I/O; and more general, context-related I/O.

The desirability of managing context information, so that a user at a workstation need not reenter information such as user identification (user ID) or patient identification (patient ID) has long been recognized.

A standard known as Health Level Seven Context Management Specification Version CM-1.1 was promulgated by the Health Level Seven (HL7) Clinical Context Object Workgroup (CCOW) on Nov. 6, 1999, incorporated herein in its entirety by reference, to define an interface and other architectural definitions of a Context Management Architecture (CMA), whereby clinical applications interact with a Context Manager to manage context information across a range of clinical and other health care related applications.

At this time, there are no other known, comprehensive context management software packages available. Some small steps have been taken for example to share context amongst one publisher's own titles, using proprietary methods absent a context manager, or to permit a user to sign onto

a single application which transfers user context to plural other applications. However, no context manager handling both user and patient context is known, much less a complete system with central administration of the context management process.

SUMMARY OF THE INVENTION

What is desired is a context administrator and method which solves the problems associated with settings using plural, unrelated software applications to process data related to a common context.

As discussed above, context is a collection of data items and corresponding values, wherein the items represent information required in common between plural applications in an industry or business setting. For example, in health care, a patient identifier (patient ID) is an item which is part of the context in which plural clinical applications may participate, or share. The data items comprising context are organized into subjects. For example, subjects defined by HL7 CCOW CM-1.1 include User, Patient and Encounter. In accordance with some aspects of the invention, a subject definition is a data structure including the following parts:

- Name (The Name must be correctly formatted per the CM-1.1 standard because attempting set the context data for an unknown subject is invalid and enforced by the context manager, as specified by the CM-1.1 standard.)
- IsSecure (If true, IsSecure indicates that only applications specifically configured to be participants to that subject can get the subjects context data. Additionally, some applications can be identified as "trusted," meaning that they can change the subject's context data, as specified by the CM-1.1 standard.)
- List of Applications (The List of Applications identifies those configured for the subject and which ones are "trusted".)
- List of Correctly Formatted Item Names for the Subject (This List gives the names of the fields that the subject is allowed to contain. Each name must be correctly formatted per the CM-1.1 standard. Each item name may be one defined in the standard or it may be formatted as a custom item name, where the format is per the CM-1.1 standard.)
- List of Dependent Subjects (One subject may be dependent on another, meaning that if the dependent subject's context is changed, this subject's context data is cleared, as specified in the CM-1.1 standard.)

On the subject of Dependent Subjects, the CM-1.1 standard has the following remarks:

For simplicity, it is generally desirable that there not be any semantic dependencies between context subjects. This enables an application to set a context subject without concern for the other available subjects.

With this assumption, it is possible for an application to independently set the context data items for just one subject, some, or all subjects during the course of a single context change transaction. A context subject whose items have not been set by the application shall remain as it was prior to the transaction.

However, in certain cases it is necessary to define and enforce semantic inter-dependencies between context subjects. The only inter-dependencies that shall be defined and enforced are those that stipulate that a specific set of additional subjects that must be set each time a particular subject is set.

For example, whenever subject X is set by an application, the application must also set subject Y. These dependencies shall be enforced by the context manager. This notion of subject inter-dependency also necessitates an additional assertion, which is that if setting X requires that Y also be set, then whenever Y is set and X is not set, the value for X shall not be post-filled by the context manager. Instead, it shall appear after the context change transaction as though X is empty.

The inter-dependencies for standard subjects are documented in the document Health Level-Seven Standard Context Management Specification, Subject Data Definitions [Ed. Note: the referenced document is part of the CM-1.1 standard.]

Inter-dependencies for custom subjects may be stipulated by the organization that defines the custom subject. A custom subject may be dependent upon any other subject. However, a custom subject may not require that a standard subject, or a custom subject defined by another organization, be dependent upon it. In other words, custom subject X can not assert that it must always be set whenever standard subject Y is set.

As used herein, context management is a process of storing, retrieving, modifying and communicating context information between a user and one or more applications, or between the plural applications used in a particular setting. For example, in health care, when a doctor switches from a heart monitor application to a blood analysis application, the patient ID need not be reentered if context management has been implemented. As used herein, context administration is a process of storing, retrieving, modifying and communicating information by which a context management system is controlled or supervised. A single context administrator may supervise multiple context managers or may supervise only one context manager.

According to one aspect of the invention, there is a method of administering a context management system, comprising configuring a subject data definition. The method may further include identifying one or more available context managers to administer. Identifying may also further include pinging possible context manager addresses to find the available context managers.

One type of data useful for security purposes is a shared secret. Thus, according to this aspect of the invention, the method may include maintaining in a subject data definition, a list or other means of identifying applications that are allowed to transact on that subject. The method may further include storing with each application a value, which is a function of, but not equal to a passcode for the application, so that the identity of an application desiring to transact on a secure subject can be verified. The method may yet further include encrypting the passcode to form the value. Methods embodying the invention can further include maintaining an inventory of applications whose context is managed; and maintaining a map relating users to user identifiers formatted for each application in the inventory. When the steps of maintaining are included, the method can also include identifying for each context, which applications share the context. In yet another variation, the method can configure communication parameters for the available context managers, generate a status report for the system or intervene in a context management process. Interventions can include forcing an application out of a context, canceling a transaction in progress or shutting down a context manager. Methods embodying aspects of the invention can include communicating with a context manager using a hypertext transport protocol. In some embodiments, the hypertext transport protocol is HTTP 1.1.

According to other aspects of the invention, embodiments thereof can include a context management and administrative system, comprising a context manager; and an administration suite. The administration suite can further include a context administrator; and a context server. The context server can further include a passcode service; a user-mapping agent (UMA) service; and a lightweight directory access protocol (LDAP) service. The LDAP service can further provide a data storage module in which the passcode service stores encrypted passcodes and in which the user-mapping agent service stores user mapping data. The context server can further include a registry in which the context manager is registered. Finally, the context server can further include configuration memory holding a common configuration used as a default configuration for the context manager.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, in which like reference designations indicate like elements:

FIG. **1** is a schematic block diagram of a system embodying aspects of the invention; and

FIG. **2** is an organizational map of one software embodiment of aspects of the invention.

DETAILED DESCRIPTION

The invention will be better understood upon reading the following description of an embodiment of our invention in connection with the drawings. This embodiment is described in connection with the administration of a software system, software components and software architecture for performing context management to synchronize a plurality of application programs to a single context. A block diagram of the embodiment is given in FIG. **1**. The illustrated embodiment complies with the HL7 CCOW CM-1.1 standard. Thus, this embodiment can perform context management in a health care environment including CM-1.1 compliant clinical applications. Other standards for context management protocols and interfaces may exist, particularly outside of health care, for which the present invention is applicable. Regardless of the existence of such standards, while the present invention is described in connection with an application of the principles thereof to the health care industry, the invention may be practiced in connection with any industry that relies on plural applications for which context can preferably be managed or synchronized.

The overall architecture of FIG. **1** is now briefly described.

One or more computer systems, workstations, desktop personal computers (PCs) or the like **100** have executing thereon one or more applications **101**, e.g., in the health care field, clinical applications. It is assumed that context management of the applications **101** is desired, and that they comply with at least one standard for context management protocols and interfaces, e.g., HL7 CCOW CM-1.1. A context manager **102**, also executing on a computer system, workstation, desktop PC or the like communicates with the applications **101** through an interface and using a protocol defined by standard. The context manager may or may not be executing on the same computer system, workstation, desktop PC or the like as the applications, but may communicate with the applications through a communications

network In the case of an HL7 CCOW CM-1 1 compliant system, Microsoft®COM protocol defines one layer of the communication protocol

Administration functions may be remote from the managed computer systems, workstations, desktop PCs, etc , for example as an independent software module or program resident on a context administration console **103**. The console **103** communicates with the system **100** on which the applications **101** reside through a channel **104** which may pass through an interconnection network, e.g., the Internet, an intranet, a Local Area Network (LAN), a Wide Area Network (WAN) or the like **105** In order to simplify communication through the interconnection network **105**, a standard printable-character based protocol, such as the Hypertext Transport Protocol (HTTP) may be used. Messages transported by HTTP may be formatted as headers, Hypertext Markup Language (HTML) files, Extended Markup Language (XML) files, etc Other protocols and message formats may alternatively be used A daemon **106**, resident on each of the systems **100**, translates the protocol used for communication over the interconnection network (e g., HTTP) into that used for context management of the applications (e.g , COM). The daemon **106** may alternatively be part of the context manager **102**

A database **107** of context information is maintained either on the context administration console or separately. When a context management installation tool **108** is invoked, similar links are established using an administration daemon **109** to draw current, common context information from the database **107**, to set up the context of newly installed applications **100**. This administration function can be performed at other times, as well, such as when a stand-alone system is brought into the context managed environment.

Although both the foregoing and the following discussion is given with respect to HL7 CCOW CM-1 1, HTTP 1 1, COM and health care clinical settings in particular, it will be apparent from the discussion that the inventors contemplate adaptations of the concepts illustrated to other industries and settings, some suggestions for which have been given

For convenience, and without loss of generality, modules, programs and machines, particularly machines executing software programs are referred to herein as modules In this document, modules could be function or procedure calls in a software program, a program module, a complete program, a machine executing a program or any part of a program, and the like, where a module performs a defined portion of the overall function of the system described.

It should be noted that the architecture described above appears to assume a particular partitioning of the context management and context administration task into individual modules, as evidenced by the blocks of FIG 1 That apparent assumption, of course, is that there is a context manager module, a context administrator module and a context server module. However, the inventors have found that the context manager and context server can be combined in a single module in which the functions are shared in such a way as to behave as a single functional block Alternatively, the context administrator and context server can be combined in a single module in which the functions are shared in such a way as to behave as a single functional block Finally, all three separately described functional elements can be combined in a single module in which the functions are shared in such a way as to behave as a single functional block. These variations have important implications for the design of the communications and user interface portions of the system because communication between more tightly coupled functional elements, such as within a module, is easier and more secure than between more loosely coupled elements, such as between modules, and because the user interface can ultimately be defined using standard elements of a page markup language interpreted by a browser, rather than a proprietary ad hoc interface design.

A context management and administration system according to a presently preferred embodiment of the invention has been implemented using the Microsoft Java programming language. The structure of the code is illustrated in FIG. 2.

A top layer, over all, is the user interface **200**. This may be implemented using a conventional presentation manager available as a resource in many operating systems, or using a markup language such as HTML or the like and HTTP so that it can use a standard browser as the display module Beneath the user interface layer, and tunneling through both lower layers is the HTTP, COM, signing and XML communication facility **201** used by all layers An inventory facility **202**, passcode facility **203** and user mapping agent facility **204**, all described below, exist in the second layer Finally, the third layer embodies the low-level functions of database management **205**, scanning the network (pinging) **206** and Lightweight Directory Access Protocol (LDAP) **207**, also all described below

The following description explains the operation of the components of the architecture described above.

The context administrator, which is connected to a communication network through which it can communicate with other elements of the system, compiles an inventory of context managers available to it on the network. The context administrator determines whether a context manager is available at each legal network address by pinging at each address a communication port registered with the Internet Assigned Numbers Authority (IANA) When a context manager is configured to respond to messages on the registered port, at the address pinged, it responds The context administrator can then build a database of available context managers The database can be presented to users in a tree form, similar to the tree used in the Windows™ Explorer program used to navigate through files and folders on a computer hard disk.

The inventory can alternatively be built and updated automatically as context managers join or leave a network. In order to do so, each context manager will register itself to the context administrator by transmitting an identifier, for example a DCE UUID, "hello" message to the context administrator. The identifier needs to be unique within a given network

As part of inventory management, a context manager can be removed from inventory, making it invisible to the context administrator A context manager manually removed by a user of the context administrator then continues to function normally, but cannot be configured, etc. by the context administrator.

Once an inventory of context managers exists, the context administrator can then configure the context managers, obtain status from the context managers, perform interventions on the context managers and produce human- or machine-readable outputs communicating various types of information about the context administration process It is also possible to view a human-readable listing of all operations performed by the context administrator. The listing is updated or appended to each time an operation is performed

Configuring the context managers is a wide-ranging task, defining how a particular instance of a context manager behaves, as well as defining site-wide information relevant to the operation of all context managers under administra-

tion. Examples of configuration parameters defining how a particular instance of a context manager behaves include the parameters related to the details of performing a transaction, such as timing parameters. Examples of configuration parameters which affect an entire site include defining which applications will join in a particular context, passcodes and other security settings, and the subjects defined by the standard, including User, Patient and Encounter, required by the standard, and optional customizable subjects.

Configuring the security settings includes defining values in a database identifying which subjects are available only through a secure connection. For example, User is a secure subject. Defining a subject as secure necessitates that trusted participants be identified, as they can only access the subject, for example for viewing or editing, provided they give the passcode identifying them as a trusted participant. In the preferred embodiment, a trusted participant is one which will be allowed to edit the contents of a secure subject. In the HL7 CCOW CM-1.1 standard, User is a secure subject.

The contents of a subject are now illustrated by describing the subject, User. The subject User is used to configure who the users are within a particular site, for example. A user mapping agent identifies each user by a unique, site-wide User Identification (User ID). The User ID is linked to the individual login identifiers, such as username and password, used to obtain access to each individual application. This map of User ID to login identifier is housed on the context server module described above.

Status information which can be obtained by the context administrator can include one or more of the version number of each context manager in the inventory, which context managers have joined a particular context, what changes have been processed by each context manager, what changes have been aborted by each context manager, etc. Status information can also include a complete record of the current configuration of each context manager, so that if a context manager inadvertently becomes out of sync with the changes made by the context administrator, as determined by making a status inquiry, that context manager can be brought back into sync. Finally, status can also include a log of exceptions which may occur from time to time during operation. The log may contain the date and time of each event, the severity of the event and a message describing the event.

In some circumstances, intervention in the operation of individual context managers may be required. The context administrator module can be configured to force an application to leave a context, cancel a transaction in progress, remotely shut down an aberrantly behaving context manager or remotely restart a context manager.

According to a preferred embodiment, all outputs of the context administrator can be printed, sorted, exported to XML, etc., so as to be available in both human- and machine-readable form.

Context changes are effected in the system by means of transactions. In the health care field, HL7 CCOW CM-1.1 defines what constitutes a transaction. According to this standard, a secure transaction occurs as follows:

This method is similar to ContextData::SetItemValues. [See CM-1.1.] The primary difference is that the context participant's digital signature shall be provided as the value of the input appSignature when secure subject item values are among the items to be set. This signature enables the context manager to authenticate that they came from a designated application or from a valid secure subject mapping agent, and that the values were not tampered with between the time they were sent and were received.

A signature is not required when the values for the user subject items are null. This enables any application to set the user context to empty. When a signature is not provided, the value of the input appSignature shall be an empty string ("").

Concatenating the string representations of the following inputs in the order listed shall form the data from which a message digest is computed by the participant:

participantCoupon

itemNames (i.e., All the elements in the order that they appear in the array)

item Values (i.e., All the elements in the order that they appear in the array)

contextCoupon

A participant shall compute its digital signature by encrypting the message digest with its private key.

The exception SignatureRequired is raised if the value of appSignature is not a digital signature and a signature is required in order to perform this method.

The exception AuthenticationFailed is raised if a digital signature is required and provided, but the process of authentication determines that: the application that invoked this method did not previously provide its public key via the interface SecureBinding; that the input appSignature has been forged; that the input parameter values have been tampered with; that the participant has not been designated for performing user context changes.

We now return to FIG. 1, to discuss how the illustrated architecture provides the facility for performing the operations described.

The context administrator module contains the logic defining the overall operation of the system. The actual maintenance and switching of context is performed by the context manager module. A variety of support functions are provided by the context server. For example, the context server may include a passcode service, a user mapping agent service and a LDAP service. These services are now discussed.

The passcode service provides a virtual software vault for the passcodes. Passcodes are stored in encrypted form in the LDAP data store accessed by the context server. Passcodes are not themselves ever transmitted as messages, but rather the context manager sends a signed HTTP message to the context server, which checks the signature and contents of the message against the stored, encrypted passcode. An MAC acknowledgement is returned to the context manager either authorizing or denying the request contained in the message.

The user mapping agent provides a similar service with respect to User IDs. A request is sent by the context manager for the login identifiers corresponding to a particular User ID, and a list of data is returned to the context manager. The context manager can then add the login identifiers corresponding to the User ID to the context data, in this case for the User subject, where it can be accessed by any application that has joined in the current context and that also has access to the User subject, which is secure.

Similarly, if the context administrator sends to the context server an LDAP message requesting a change to the passcode list or the map of User ID information, a security check is first performed, and then the transaction is either approved or disapproved.

The context server could be used to provide other services, as well. For example, the context server could provide a registry service, in which each context manager is registered. The registry would automate the inventorying process to a greater extent, allowing context managers and context

servers to perform a handshake when a new module comes on line on a network, and the context manager to be automatically registered. The context administrator could also provide a default configuration service. Each registered context manager could be configured to the default configuration at the time it is registered, unless the default configuration is overridden.

The context server can be implemented as a server appliance. A server appliance is a network-connected server that services multiple client computers. Like conventional servers, a server appliance receives requests from client computers to perform specific tasks. The server performs a task requested and returns back to the client the result of performing the task. Unlike conventional servers that provide general purpose platforms for a wide range of computing tasks, a server appliance is singular in purpose. A server appliance contains specialized software and possibly specialized hardware to enable it to achieve its purpose. Thus, a server appliance can be optimized for the specific tasks that it is intended to perform, thereby reducing the cost and complexity of the server appliance when compared with the cost and complexity of a general purpose server configured for the same purpose.

The context administrator inventories the network by pinging all possible context manager addresses on a port registered with the IANA, according to one embodiment of the invention. The context administrator can be implemented on a Windows™ 98/2000/NT machine, and use the Windows™ Networking ping function to perform the required scan. Other operating systems such as Unix, Linux and the like, with their corresponding networking facilities can also be used.

According to some embodiments of the invention, communication between the context administrator and the context manager can occur using HTTP. However, context managers communicate with applications using the COM protocol, as mentioned above.

Therefore, in these embodiments of the invention, rather than add to the complexity and size of the context manager, a software daemon translates between HTTP and COM protocols. The context administrator sends signed messages to the context manager in HTTP, which are translated by the daemon into signed COM messages. The context manager returns XML messages, which the daemon wraps in HTTP to forward to the context administrator. Naturally, other communications protocols can be used, and even the native protocol used by the context manager can be used directly, in variations on embodiments of the invention.

It should be noted that for security reasons, the daemon is restricted to calling only COM objects which are part of the context manager module. Theoretically, an HTTP request could be for any COM object, but that would create a security breach by allowing the daemon to be used to gain access to other system components.

In order to effect proper communication between the context managers and the context servers, one configuration parameter set in the context managers is which context server, of a possible plurality on a given network, should be used. A failover mechanism can also be provided which would cause a secondary context server to be used in the event a primary context server failed to respond to a message.

Based upon the foregoing architecture, a new subject is implemented by the context administrator as follows. First the subject is defined in the context administrator by giving it a name and defining its schema. The definition is stored in the repository. Next, a user gestures to send out the configuration, causing an HTTP call to the context manager, through the daemon, to be sent out. Alternatively, the configuration can be stored in a context server in a configuration service, as discussed above. Finally, the context manger obtains and stores the new configuration information locally in a text file. This discussion, of course, assumes that one or more applications controlled by the context manager have a priori knowledge of the new subject, thus giving life and meaning to the new subject definition. If the subject has been defined to be secure, then the application will need a passcode to use the subject. Also, any new subject definition must have at least one application capable of setting data in the subject.

In one variation of the invention, the context manager can be embodied in a server appliance, as described above in connection with the context server. In such an embodiment of the invention, the applications may reside in a different computer, workstation, PC, etc. than the context manager appliance, which also may reside in a different computer, workstation, PC, etc. than the context administrator. The components of such a system which reside in different computers, workstations, PCs, etc. would be connected to each other through a network, such as a LAN, a WAN, an intranet, the Internet, etc.

In other variations of the invention, the structures and methods described herein can be combined with: the context sensitive web casting methods and apparatus disclosed in U.S. patent application Ser. No. 60/135,907, filed May 25, 1999, incorporated herein in its entirety by reference; the context management server appliance methods and apparatus disclosed in U.S. patent application Ser. No. 60/136,670, filed May 28, 1999, incorporated herein in its entirety by reference; the healthcare server appliances methods and apparatus disclosed in U.S. patent application Ser. No. 60/139,235, filed Jun. 14, 1999, incorporated herein in its entirety by reference; the HTTP Post message encoding of COM dispatch interface calls disclosed in U.S. patent application Ser. No. 60/139,145, filed Jun. 14, 1999, incorporated herein in its entirety by reference; the application context management methods and apparatus disclosed in U.S. patent application Ser. No. 60/146,722, filed Aug. 2, 1999, incorporated herein in its entirety by reference; and the context management web site methods and apparatus disclosed in U.S. patent application Ser. No. 60/145,681, filed Jul. 26, 1999, incorporated herein in its entirety by reference. This discussion and that contained in the referenced patent applications clearly suggest to the skilled artisan how such combinations would be made.

The invention has now been described and illustrated in connection with one embodiment and some variations thereof. Numerous other variations and modifications which will now be obvious to the skilled artisan are also contemplated as within the scope and spirit of the invention. The scope of the invention is not to be limited by the description of embodiments thereof, but only by the scope of the properly construed claims which follow.

What is claimed is:

1. At least one computer readable medium encoded with a program that, when executed, performs a method of administering a context management system that manages a context, the method comprising:

configuring a subject data definition which defines a plurality of subjects in the context using, for each subject, subject data that comprises a data item usable by a plurality of applications comprising at least a first application and a second application, the data item having a set of values comprising at least a first value

corresponding to the first application and a second value corresponding to the second application, the set of values identifying the subject in the context, the value of the data item corresponding to the first application being exchangeable with the value of the data item corresponding to the second application when a user switches from the first application to the second application to retain the context, the plurality of subjects comprising a patient subject, a user subject and an encounter subject, and the subject data definition being defined in accordance with a Clinical Context Object Workgroup (CCOW) standard.

2. The at least one computer readable medium of claim 1, wherein the method further comprises:

identifying one or more available context managers to administer.

3. The at least one computer readable medium of claim 2, wherein identifying further comprises:

pinging possible context manager addresses to find the available context managers.

4. The at least one computer readable medium of claim 1, wherein the method further comprises:

maintaining in the subject data definition, information identifying which applications are allowed to access the subject.

5. The at least one computer readable medium of claim 4, wherein the method further comprises:

storing with each application a value which is a function of but not equal to a passcode for the application

6. The at least one computer readable medium of claim 5, wherein the method further comprises:

encrypting the passcode to form the value

7. The at least one computer readable medium of claim 1, wherein the method further comprises:

maintaining an inventory of applications whose context is managed

8. The at least one computer readable medium of claim 7, wherein the method further comprises:

maintaining a map relating User IDs to login identifiers formatted for each application in the inventory.

9. The at least one computer readable medium of claim 2, wherein the method further comprises:

configuring communication parameters for the available context managers.

10. The at least one computer readable medium of claim 2, wherein the method further comprises:

generating a status report for the system

11. The at least one computer readable medium of claim 2, wherein the method further comprises:

intervening in a context management process.

12. The at least one computer readable medium of claim 11, wherein intervening further comprises:

forcing an application out of a context.

13. The at least one computer readable medium of claim 11, wherein intervening further comprises:

canceling a transaction in progress.

14. The at least one computer readable medium of claim 11, wherein intervening further comprises:

shutting down a context manager

15. The at least one computer readable medium of claim 1, wherein the method further comprises:

communicating with a context manager using a hypertext transport protocol

16. The at least one computer readable medium of claim 15, wherein the hypertext transport protocol is HTTP 1.1.

17. An apparatus comprising:

at least one processor programmed to manage and administer a context, the at least one processor programmed to implement:

a context manager; and

an administration suite for configuring a subject data definition, the subject data definition defining a plurality of subjects in the context using, for each subject, subject data that comprises a data item usable by at least a first application and a second application, the data item having a set of values comprising at least a first value corresponding to the first application and a second value corresponding to the second application, the set of values identifying the subject in the context, the value of the data item corresponding to the first application being exchangeable with the value of the data item corresponding to the second application when a user switches from the first application to the second application to retain the context, the plurality of subjects comprising a patient subject, a user subject and an encounter subject, and the subject data definition being defined in accordance with a Clinical Context Object Workgroup (CCOW) standard

18. The apparatus of claim 17, wherein the at least one processor is programmed so that the administration suite further comprises a context administrator and a context server.

19. The apparatus of claim 18, wherein the at least one processor is programmed so that the context server implements:

a passcode service;

a user mapping agent (UMA) service; and

a lightweight directory access protocol (LDAP) service.

20. The apparatus of claim 19, wherein the at least one processor is programmed so that the LDAP service further comprises:

a data storage module in which the passcode service stores encrypted passcodes and in which the user mapping agent service stores user-mapping data.

21. The apparatus of claim 18, wherein the at least one processor is programmed so that the context server further comprises:

a registry in which the context manager is registered

22. The apparatus of claim 18, further comprising at least one storage device, and wherein the at least one processor is programmed so that the context server further comprises:

a configuration memory, in the at least one storage device, holding a common configuration used as a default configuration for the context manager.

23. The apparatus of claim 17, wherein the at least one processor comprises a single processor programmed to implement the context manager and the administration suite.

24. The apparatus of claim 17, wherein the at least one processor comprises at least a first processor programmed to implement the context manager and at least a second processor programmed to implement the administration suite.

25. The apparatus of claim 17, wherein the at least one processor is programmed so that the administration suite generates a log which includes information received from the context manager

26. The apparatus of claim 17, wherein the log comprises an indication of a processing exception observed by the context manager.

27. The apparatus of claim 17, wherein the at least one processor is programmed so that the administration suite, subsequent to configuring the subject data definition, reconfigures the subject data definition, and communicates the reconfiguration of the subject data definition to the context manager.

28. The apparatus of claim 17, wherein the at least one processor is programmed so that the administration suite generates an inventory which includes the context manager.

29. The at least one computer readable medium of claim 2, wherein the method further comprises:

generating a log which includes information received from at least one of the available context managers.

30. The at least one computer readable medium of claim 29, wherein the act of generating the log comprises generating a log which includes an indication of a processing exception observed by the at least one of the available context managers.

31. The at least one computer readable medium of claim 2, wherein the method further comprises:

subsequent to the act of configuring the subject data definition, reconfiguring the subject data definition, and communicating the reconfiguration of the subject data definition to at least one of the available context managers.

32. The at least one computer readable medium of claim 2, wherein the method further comprises:

generating an inventory of the available context managers to administer.

* * * * *

SCHEDULE B

DEFINITIONS

The definitions listed in Schedule A are hereby incorporated by reference.

DEPOSITION TOPICS

DEPOSITION TOPIC NO. 1

The authenticity of the documents and things produced by Duke University Medical Center in response to Schedule A.

DEPOSITION TOPIC NO. 2

Duke University Medical Center's policies and practices with respect to the preparation and retention of documents and things of the type produced by Duke University Medical Center in response to Schedule A.

DEPOSITION TOPIC NO. 3

The circumstances under which the documents and things produced by Duke University Medical Center in response to Schedule A were created or prepared including, but not limited to, whether the documents and things were prepared at or near the time of the acts, events, conditions, opinions or diagnoses recorded by, or from information transmitted by, a person with knowledge, whether the documents and things were kept in the course of a regularly conducted business activity, and whether it was the regular practice of Duke University Medical Center's business activity to make the documents and things.

DEPOSITION TOPIC NO. 4

The development of any CCOW enabled context manager by Duke University Medical Center prior to December 11, 2001.

DEPOSITION TOPIC NO. 5

The development of the CCOW standard.

DEPOSITION TOPIC NO. 6

The work performed at Duke University Medical Center or on behalf of Duke University Medical Center with regard to the development of the CCOW standard, including all versions thereof, or its predecessor(s) or any other standard or protocol involving context management in healthcare information systems including, but not

limited to, all such work performed, directed by, or participated in by W. Edward Hammond.

DEPOSITION TOPIC NO. 7

The development and or activities of the Visual Integration Research Center.

DEPOSITION TOPIC NO. 8

The state of the art of the subject matter of the '313 and '556 patents as of December 11, 2000 and April 7, 1999 respectively.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Kenneth L. Dorsney, hereby certify that on October 30, 2006, the attached document was hand-delivered to the following persons and was electronically filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following and the document is available for viewing and downloading from CM/ECF:

Frederick L. Cottrell, III
K. Tyler O'Connell
Richards Layton & Finger
One Rodney Square
P.O. Box 551
Wilmington, Delaware 19899

I hereby certify that on October 30, 2006, I have Electronically Mailed the documents to the following non-registered participants:

Matthew B. Lowrie
Aaron W. Moore
Lowrie, Lando & Anastasi, LLP
Riverfront Office Park
One Main Street – 11th Floor
Cambridge, Massachusetts 02142
mlowrie@ll-a.com
AMoore@ll-a.com

By: */s/ Kenneth L. Dorsney*
Richard L. Horwitz
Kenneth L. Dorsney
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, Delaware 19899-0951
(302) 984-6000
rhorwitz@potteranderson.com
kdorsney@potteranderson.com

726216